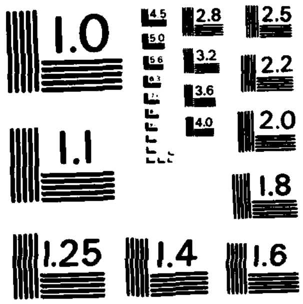
AD-A132 888 COMPUTERS ON THE BATTLEFIELD: CAN THEY SURVIVE?(U)
NATIONAL DEFENSE UNIV WASHINGTON DC RESEARCH
DIRECTORATE R J DEBASTIANI 1983
UNCLASSIFIED NATL SEC AFFAIRS MONO SER-83-5 F/G 9/2 NL

1/2




MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

COMPUTERS ON THE BATTLEFIELD: CAN THEY SURVIVE? DEBASTIANI

AD-A132 888

monograph series no. 83-5

(5)

# COMPUTERS ON THE BATTLEFIELD

## CAN THEY SURVIVE?

RICHARD J. DEBASTIANI



the national defense university

NDU PRESS

## NATIONAL DEFENSE UNIVERSITY

**Lieutenant General John S. Pustay, USAF**
**President**

## The Research Directorate and NDU Press

**Director of Research and Publisher**
Colonel John E. Endicott, USAF

**Associate Director and Professor of Research**
Colonel Frederick T. Kiley, USAF

**Deputy Director, Plans and Programs**
Major William A. Buckingham, Jr., USAF

**Deputy Director, Administration**
Lieutenant (Junior Grade) Pearl M. Moriwaki, USN

**Deputy Director, Production**
Major Donald Anderson, USAF

**Senior Editor**
George C. Maerz

**Writer-Editors**
Evelyn Lakes
Janis Hietala
Rebecca W. Miller
Albert C. Helder

**Executive Secretary**
Anne Windebank

**Editorial Clerks**
Pat Williams
(Lead Clerk)
Dorothy M. Mack
Carol A. Valentine

**Office Manager**
Laura W. Hall

**Office Assistants**
Hattie Johnson
Cecelia Giles

# COMPUTERS ON THE BATTLEFIELD

## Can They Survive?

by

A

Colonel Richard J. DeBastiani, USA
Senior Research Fellow

National Security Affairs Monograph Series 83-5
1983

National Defense University Press
Fort Lesley J. McNair
Washington, DC 20319

## NATIONAL SECURITY AFFAIRS MONOGRAPH SERIES

The National Defense University (NDU) Press publishes a monograph series in order to circulate NDU research on selected aspects of national security policy. The monograph series presents the research findings of senior fellows, faculty, students, and associates of the University and its component institutions, the National War College, the Industrial College of the Armed Forces, and the Armed Forces Staff College. In addition to these monographs, the NDU Press publishes the National Security Essay Series, books, issue papers, reports, and conference proceedings.



*Order Information.* Additional printed copies of NDU Press publications are sold by the Superintendent of Documents, US Government Printing Office (GPO), Washington, DC 20402. Order directly or through your local GPO bookstore. NDU Press publications are also sold in facsimile copy: registered users should contact the Defense Technical Information Service, Cameron Station, Alexandria, VA 22314; the general public should contact the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

## DISCLAIMER

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author(s), and do not necessarily represent the views of the National Defense University, the Department of Defense, or any other Government agency.

## DISTRIBUTION STATEMENT

Cleared for public release; distribution unlimited.

For sale by the Superintendent of Documents, U S Government Printing Office, Washington, DC 20402

# CONTENTS

# FOREWORD

The survival of computer systems may well prove critical to the success or failure of US military forces in combat. Survivability of computer systems is a new issue, one about which little has been written. Now that information and experience gradually have become available, the national defense community must begin to address the major problems posed by this new technology.

In this ~~pioneering~~ effort, Colonel Richard J. DeBastiani, US Army, examines the factors affecting computer survivability in both conventional and nuclear land battles. ~~He~~ explains the necessity of including survivability as a key consideration in the peacetime development, standardization, training, management, and procurement of computer resources. He concludes by examining a mature Army computer system for lessons that planners can apply to the design of future systems.

Given the continuing proliferation of computer technology throughout our armed services, this study of computer survivability is indeed timely. The National Defense University is pleased to offer this analysis to those concerned with the many problems of integrating computers into US military forces.

Accession For

John S. Pustay
Lieutenant General, USAF
President, National
Defense University

A

# ABOUT THE AUTHOR

Colonel Richard J. DeBastiani, United States Army, wrote this monograph while a Senior Research Fellow with the National Defense University. He is a graduate of the National War College and the Industrial College of the Armed Forces and holds a bachelor of science degree from Indiana University of Pennsylvania and a master's degree in Business Administration (Operations Research) from Tulane University. Colonel DeBastiani has lectured at George Washington University, the National War College, and the Industrial College of the Armed Forces. He is now the Director of Operations Analysis at the Army Logistics Center. Colonel DeBastiani's other assignments include commanding a Support Battalion, a Supply and Transport Battalion, and a Material Management Center in the 25th Infantry Division, managing the development of manpower planning and programing models and computer systems for the Assistant Secretary of the Army for Manpower and Reserve Affairs, and analyzing logistic systems in the operational and combat developments arenas.

# PREFACE

Computers increase the combat power of a force by processing information faster and more accurately. Soon, commanders will be able to decisively commit and direct forces by using computerized command and control systems. Clearly, there is a trend in the Army toward an automated battlefield, yet the Army must be cautious in its automation endeavors because current computers cannot survive nuclear or chemical attack. They are vulnerable to electromagnetic pulse (EMP) and persistent chemicals. Thus, Army reliance on these computers must be tempered while initiatives making computers more survivable on the battlefield are developed and implemented. In this monograph I have tried to identify the major issues which play a role in determining computer survivability on the battlefield. For these issues, I have recommended a number of specific actions to improve computer system survivability.

This study serves three audiences. *Congress and industry* are informed of the factors that influence computer survivability and of the necessity to develop a military computer family that can be repaired and operated by Army personnel. Chapter 1 speaks directly to this audience. *Defense and Army policy officials* are made aware of the key issues, with recommendations to make computers more survivable on the battlefield, in chapter 4. *Developers and designers of battlefield automated systems* should be interested in the entire monograph.

This research would not have been possible without the help and cooperation of personnel from the Army Logistics Center of the Communications Electronics Command, DARCOM, and the Army Staff. I'm deeply indebted to Colonel Fred Kiley of the National Defense University for his guidance and criticism throughout my research and for his efforts to publish this monograph.

Since this document is independent research, I assume responsibility for any errors or omissions. The views and recommendations of the monograph are my own and do not necessarily reflect US Gov-

ernment policy or represent the views of the National Defense University, the Department of Defense, or any other Government agency.

**RICHARD J. DEBASTIANI**

# EXECUTIVE SUMMARY

What are the actions the Army should take to make its computer systems more survivable? Two baseline actions are required—harden the computers or the shelters that house them and create redundancy on the battlefield through computer standardization.

Thirty-nine recommendations expand on these baseline actions by specifically identifying organizational, personnel, training, and logistical policy changes required to make Army computer systems more survivable on the battlefield. The key recommendations focus on standardization—one military computer family for all functions on the battlefield, one organization (the Department of the Army Materiel Development and Readiness Command) to design computer systems, one regulation for buying computers, and one focal point (the Under Secretary of Defense Research & Engineering) for computers at the Department of Defense. Of these recommendations, the most important is establishing the military computer family (MCF). According to one estimate, MCF will not only save $1 billion over our current method of doing business by 1993 but will also enable the Army to provide to its field commanders more flexibility with better support. With MCF, one regulation, and one organization providing central direction, all facets of computer training, repair, and replacement are easier. Another major recommendation is placing trained personnel where they are needed. Authorization documents and personnel requisitioning procedures must be changed to reflect the requirement for specially trained personnel. Only then can the Army match its personnel forces with its space authorizations.

These suggestions, combined with the other monograph recommendations, will put the Army on a path to achieve survivable battlefield computer systems.

# INTRODUCTION
# WHY STUDY COMPUTERS?

In a 1981 *Armed Forces Journal* article, an Army observer estimated that battlefield automation from 1981 to 1985 will cost the Army over $22 billion (in then-year dollars).[1] Translated into today's dollars, the figure is even more impressive, yet this investment in automation does not guarantee the Army's computers will function on the battlefield. In a nuclear and chemical environment, Army computers are not survivable, for the most part; in conventional war the computers, although vulnerable, can survive. Conventional war vulnerabilities are aggravated by current and planned computer proliferations to virtually all functional units.

Current computer policies hamper the US Army's ability to effectively adapt computer technology to the battlefield. Yet, without this technology the US Army would resemble an underdeveloped nation's army of the past—led by the horse cavalry instead of the air cavalry. The Army cannot ignore computer technology. Instead, the Army must harness and adapt the computer to battlefield use by changing policies until the Army is as comfortable with the computer as it is with the radio.

Imagine a highly sophisticated computer on a future battlefield responding to a voice command, analyzing a myriad of intelligence data from a variety of sources (satellite, radio, etc.), and providing the commander near real-time intelligence updates on enemy forces. In this role the computer could serve as a force multiplier, but it could also create havoc on the battlefield if the data it produced were assumed to be infallible.

## STUDY BOUNDARIES

This study has an underlying central question: Does using the computer in combat aid or hinder the Army in defeating the enemy? To bound this question, the analysis is limited to battlefield computers (computers used in the direct support of the corps and division). Although many of the comments throughout this study are applicable to computers embedded in weapons systems, this evaluation of Army computer systems is directed toward general purpose computers used in logistics, administration, and command and control systems.

## STUDY CONTENTS

Three chapters, a concluding chapter, and an appendix make up this study. (The appendix serves as a case in point.) This report examines and evaluates concerns and, in its conclusion, identifies issues and gives recommendations to resolve the issues. A synopsis of the chapters and the appendix follows:

- Chapter 1 identifies the environmental and system factors that influence the survivability of a computer system. This chapter contains two key thrusts. The first looks at how nuclear and chemical environments affect computer systems and their components (shelters, communication, and computer equipment). The second inquiry examines the impact of Army's policies for buying, maintaining, and standardizing computers on the survivability of the computer on the battlefield under any wartime condition.

- Chapter 2 reviews the progress made in command and control function automation and evaluates the need to automate command and control systems.

- In chapter 3 the lessons learned from the supply system case in point are applied to the Army's development of its automated command and control systems to determine the degree of success the Army has had in applying lessons learned to new system developments.

- Chapter 4 lists seven issue areas and recommends actions.

• The appendix is a case study of a mature 20-year-old Army computer system, the theater supply system. In this appendix, factors that influence computer system survivability are used to identify lessons in the development and fielding of the theater supply system—a system that must be capable of making the transition from a peacetime to a wartime environment. Discussions center on computer use, on manning computer organizations, and on training personnel to operate the computers located in the theater. The appendix concludes with alternatives for making the supply system more survivable in war.

# 1. AN ELECTRONIC BEACHHEAD: COMPUTER SYSTEMS SURVIVABILITY

Thoughtful and detailed preconflict planning prevents periods of confusion, doubt, and indecision in times of war. For the Army, planning for computer systems efficiency and survivability must address (1) the nuclear, biological, and chemical (NBC) environment; (2) the shelters that house and protect the computers; (3) the communications that transmit information from one point to another; and (4) our ability to operate, maintain, standardize, and distribute computer equipment on the battlefield. Each of these factors affects computer survivability.

The following analysis of these factors is limited to the computers used by the Army in a theater of operations.

## THE NBC ENVIRONMENT

The NBC environment can be likened to Cerberus—with all three heads (the nuclear, the biological, and the chemical) posing threats. (In mythology, Cerberus is a three-headed dog guarding the infernal regions.) In the event that this environment must be faced, there is a US policy on NBC warfare, a policy which is basically defensive. Briefly, our policy as contained in Army Field Manual 21-40 is this:

- Nuclear weapons will be used as a last resort, considered only after all conventional means of warfare have been severely tested and found to be inadequate, or they will be used in response to threats of the enemy's first use. Authority for nuclear weapons use rests with the President.

- Toxins or any other method of biological warfare will not be used under any circumstances.

• Chemical agents, lethal or incapacitating, will not be used by US forces first; however, the United States reserves the right to retaliate against an enemy force which has used them on US forces. Authority for the first retaliatory use rests with the President.

The following review will focus on the nuclear effects and to a lesser extent on the chemical effects on computers. Meaningful information and completed studies of biological effects on electronics are virtually nonexistent.

**NUCLEAR**

Four types of nuclear explosions—high altitude, low altitude, surface, and subsurface blasts—can affect computer systems and computer electronics. Depending on the type of explosion, each nuclear detonation generates varying degrees of heat, radiation, electromagnetic pulse (EMP), and shockwave—each of which uniquely affects computer electronics. We tend to think of a nuclear explosion in terms of thermal effects (heat), radiation, and blast (shock wave); however, EMP has emerged as the Army's major problem to overcome in a theater nuclear war.[1] (Thermal radiation, nuclear radiation (neutron and gamma rays), and blast are generated by air or surface bursts. Their impact on computer equipment survivability depends on the size and distance of the burst from the computer. Electromagnetic pulse, an energy source similar to a lightning bolt but many times greater, is created by the interaction of nuclear radiation (from a nuclear burst) with ions in the atmosphere, or the atmosphere and the earth's surface.)

The nuclear survivability equation includes another variable, personnel, which must be considered when examining equipment survivability. Because personnel are vulnerable to nuclear radiation, thermal radiation, and the blast effects of a nuclear detonation, equipment survivability need only equal the operator survivability rate.[2] Beyond this it becomes pointless to spend huge sums in engineering and high developmental costs in computer equipment design. This study of computer survivability does not define the "thin red line," and the correlated characteristics, where enough of the crew have survived a nuclear detonation to ensure continued computer

operations. Comments on blast, thermal radiation, and nuclear radiation assume operator survivability.

In order to protect computer equipment against the shock wave created by a nuclear blast, all equipment in the shelter must be shock mounted. Thermal radiation, or heat, poses only a minor threat to today's computers, attacking the Mylar, rubber, and plastic components (tape, discs, cables, etc.) in the peripheral equipment. Trends in computer technology are vaulting toward fiber optics (a system using transparent glass material—similar to a glass pipe that conducts or guides light through thinly constructed glass strands). Fiber optics are sensitive to thermal radiation, which darkens the glass pipes and chokes off the light. Without this light, data do not flow through the computer, and information output churns to a standstill. In tomorrow's computers, heat, because of its effects on fiber optics, may prove to be a significant problem.

The other aspects of nuclear explosion (gamma rays, neutrons, and X-rays—the radiation) affect computers much more than blast or heat, particularly if the nuclear detonation should occur within a 3-kilometer radius of the computer. Within this radius the transient effects on electronics (TREE) can cause burnout by fusing the closely meshed microcircuits of electronic components. Before the integrated circuit, the TREE effects were truly transient; that is, the component would stop functioning only while the radiation was passing through the electrical component. Electrical components in the 1960s consisted of vacuum tubes and loosely packed transistors. With the more recent medium- and large-scale integrated circuit technology, the radiation permanently burns out the closely packed transistor circuits in the silicon chip.

When an electrical component is burned out by TREE or by EMP, the component itself also generates an electromagnetic pulse called system-generated electromagnetic pulse. Because the computer equipments in the shelter or fixed facility are physically located close together, system-generated electromagnetic pulse can affect the computer components in the same manner as EMP. Because newer circuits are less EMP resistant, the significance of EMP over the last 20 years has greatly increased. Circuits evolved from EMP resistant vacuum tubes to more vulnerable transistors, to highly vulner-

able small-, medium-, large-, and very large-scale integrated circuits. The more compact the circuitry becomes the greater its vulnerability to EMP, and technological progress continues to produce more compact microcircuitry. These advances, ironically, could be self-defeating. Department of Defense research and development in very high speed integrated circuits (VHSIC), which pack circuits even more closely together, will make computers more vulnerable to EMP unless the VHSIC community can find a solution to the EMP problem.

Electromagnetic pulse creates a voltage surge in electronic components. Every electrical cable, antenna, or orifice protruding from electrical components will absorb this voltage pulse to varying degrees unless adequately shielded. Table 1-1 shows how powerful EMP is compared to the power normally handled by other electrical components. Visualize the destructive power of one million watts penetrating a microcircuit—phzzth!

**Table 1-1. Electromagnetic Energy Comparison**

| **Power/Energy Source** | **Power Density (Watts/Square Meter)** |
|---|---|
| Typical radio receiver | 0.001 |
| Typical radio transmitter | 100 |
| Directional pulse radar | 1,000 |
| EMP | 1,000,000 |

*Source:* US Army Nuclear Agency, *note no 1 on* EMP, June 1974.

Although EMP engulfs electronic equipment, particularly micro electronic components, EMP is harmless to personnel. Nevertheless, commanders, computer operators, and analysts should understand EMP effects in order to operate computer systems that will function effectively in a nuclear war.

Table 1-2 compares EMP effects of various-size nuclear detonations. The higher the detonation and the higher the yield, the greater the EMP effect on the earth's surface.

An air burst 200 miles up can effectively inundate a theater of operations with EMP. Without a deliberate effort to de-

**Table 1-2. Nuclear Explosion EMP Effect on the Earth's Surface**

| Nuclear Burst (10 Megatons) | EMP Ground Radius Effect |
|---|---|
| Subsurface | Less than 1 mile |
| Surface | 2–5 miles |
| Air—19 miles up | 9 miles |
| Air—50 miles up | 600 miles |
| Air—100 miles up | 900 miles |
| Air—200 miles up | All of the US and parts of Mexico and Canada |

*Sources:*

Eric J. Lemer, contributing ed., military electronics, "Electromagnetic Pulses: Potential Crippler," *IEEE Spectrum* 18 (May 1981): 41–46.

Janet Raloff, "EMP—A Sleeping Electronic Dragon," *Science News* 119 (9 May 1981): 301.

US Army Nuclear Agency, note no. 1 on EMP, June 1974.

sign and shelter computers against EMP, theater computers (mobile and fixed) will cease to generate critical information required for timely, functional decisions. Computer memories and electronic components would, in many cases, be permanently damaged. Information stored on peripheral equipment, such as tapes and discs, would be destroyed only if the tape or disc were in a read or write mode. Although tests have shown that magnetic tape is not sensitive to high levels of EMP, the central processor is highly susceptible to permanent EMP damage.[3]

In spite of the danger, actions can be taken to protect equipment and lessen the effects of high-altitude EMP (HEMP) on computer electronics. HEMP protective alternatives should concentrate on blocking the electromagnetic energy from reaching the electronic components of the computer, on making electronics resistant to transient effects, and on making the electronics systems fault tolerant. These are alternatives which are achievable through hardware and software design modifications. The hardware approach to hardening computer systems focuses on shielding, voltage and current delimiters (filters, suppressors, and energy absorbers), grounding and bonding systems, and the duplication of system units to provide equipment redundancy. On the other hand, software approaches to lessening the effects of

EMP should provide for plausibility (feasibility) checks on input and internal data and processes, such as the following:

- An operating system executive function (interrupt handling, storage allocations, timing and process scheduling).
- Fault detection, reporting, and automatic recovery programs (checkpoint restarts and program and data rollouts).
- Fault tolerant software (system and communications protocols).
- System monitoring, traffic priorities, and resource allocations.[4]

These checks would enable the data to be reconstructed following EMP with minimum system degradation. Whatever the approach—hardware, software, or both—undertaken to modify Army computer systems to negate EMP, it should be affordable.

In addition to the computer and its peripherals, power sources are subject to EMP. Look at the equipment which provides power to the computer. Where does the computer get its power—from an external source such as Con Edison or a field generator? Both sources, commercial power and field generators, are vulnerable to EMP. Thus, design requirements need to include all elements of the computer system—the shelter, those components in the shelter, and the power sources outside the shelter. Since all Army computers are vulnerable in varying degrees to EMP, we must design computer systems (hardware and software) with EMP in mind.

## BIOLOGICAL

To continue the analogy, Cerberus' second head represents the possible dangers of biological warfare to computer equipment and personnel. Compared to the subjects of nuclear and chemical warfare, considerably less work has been initiated and virtually none completed on determining the effects of biological events on electronics. Because the Soviet Union and its allies are using chemicals and biological agents in Afghanistan, Kampuchea, and Laos,[5] the United States has

cause to initiate research on the effects of toxins on electronics.

## CHEMICAL

The concept of chemical survivability is similar to that of nuclear survivability—making equipment survivable against chemicals only to the point at which enough personnel survive to operate the computer and continue the unit's assigned mission. Until recently, research into this third head of Cerberus had been very limited. Within DOD, computer procurement specifications for chemical survivability have been virtually nonexistent. As of 1 January 1982 no regulation existed requiring equipment to be made survivable against chemical attack.

Two major areas of concern have surfaced on computer survivability during chemical attack. First, computer operators cannot physically operate computers effectively in a maximum mission-oriented protective posture (MOPP)—the chemical protective battle dress. A lighter weight garment is needed. Secondly, once the chemical enters the shelter and the computer, no prescribed procedures exist for decontaminating the computer or its peripherals (tapes and discs). For decontamination purposes, chemicals can be categorized as persistent and nonpersistent chemical agents. Choking (CG) and blood (AC and CK) agents are nonpersistent agents, while nerve (VX and GD) and blister (HD and L) agents are persistent. Russian nerve agents are thickened. (When thickened, the nerve agent becomes more persistent causing a greater decontamination problem in electronic components.) More research should be conducted by the Army to develop substance and procedures for decontaminating electronic equipment.

One approach to protecting equipment from chemical agents is ensuring the chemical remains isolated from the computer. Isolating chemical agents from the computer will be discussed under shelters, following.

## SHELTERS

Nowhere is the Army's struggle with planning more evident than in the deficiencies of our shelters. A primary objec-

tive of a shelter should be protecting the equipment and personnel housed within the shelter. Unfortunately, current shelter designs lack adequate protection against an NBC threat. Deficiencies in shelter design range from poor filters on air conditioners (for stopping radiation fallout) to no forced air pressure system (for keeping contaminants from entering the shelter). Also unfortunately, forced air pressure systems will not decontaminate dirty personnel or material contaminated with persistent agents being brought into the shelter. Not until 7 April 1981 did the Army hold a conference to determine the extent of the Army's shelter problem. That conference, at the US Army Logistics Center, confirmed that current shelters provide negligible NBC protection. These deficiencies indicate a major problem in shelter development—the failure to look at the total system, the shelter, the power source, and the vehicle that carries the shelter.

One alternative to shelter deficiency requires the retrofitting of existing shelters to make them more protective in an NBC attack. Shelter development was not coordinated with vehicle development. This means that shelters positioned on vehicle carriers exceed maximum carrying weights. For example, at a cost of about $60,000, the S-250 shelter for the 5/4-ton truck can be hardened, but it will exceed the weight carrying capability of the truck. In fact, without shelter hardening, the 5/4-ton truck with shelter is near its maximum load carrying capacity. Trucks exceeding their load carrying capacities would be maintenance nightmares in peacetime. Imagine the problem these trucks would cause in wartime.

Another alternative protection against radiation fallout and chemical agents and toxins is developing modified collective protection equipment. This development entails designing a portable protective entrance which, when attached to the shelter, would pass filtered air under pressure over the soldier to decontaminate the individual for nonpersistent agents before entering the shelter. If this equipment is to be useful, it should be relatively light and easily assembled and disassembled for rapid unit displacement.

According to the attendees at the Logistics Center conference mentioned earlier, the current collective protection equipment was designed with little consideration for standard

power sources. Shelters with collective protection equipment require a 400-hertz power source; this means the collective protection equipment cannot be mounted on 1½- and 2½-ton vehicles and use the vehicle's batteries on the generator which provides power to the electronic equipment housed in the shelter.

All of the above indicate that our future shelter program should ensure that (1) requirements are developed, (2) doctrine is authored for publication and dissemination, and (3) the total system is considered in the development process. In addition, our shelters and those of our allies should be compatible. To ensure interoperability, the United States must have minimum standards of technical specifications with its allies. NATO and US shelters should protect computer operations against the NBC threat. At present, OSTAG 44 (NATO regulatory requirements) and the US hardened tactical shelter program specifications are not entirely compatible. They should be.

## COMMUNICATIONS

How do communications affect computer survivability? The relationship between the computer and communication is direct in a distributive computer system. (The distributive computer system is a computer network with a set of computer systems and terminals that are connected by communications equipment whereby the distributed system shares the computers or database or both.) Without communication, distributive computer systems are inefficient and ineffective. Subsequent insufficient or untimely information may force the decision-maker to make premature or incorrect decisions. In command and control systems, this can mean the difference between winning or losing. For example, in the European theater, information is passed over military and commercial communications media (such as wire, radio, microwave, or satellite). The military and commercial electronic equipment used to transmit and receive this information is affected by the NBC environment in much the same manner as computers. HEMP is a major problem for communication-electronic components. However, nuclear detonations generate different problems with radio communications, often an integral link of a telecommunications net. (Teleprocessing equipment ties the computer

to this telecommunications net.) Depending on the type of burst and mode of communications propagation, blackouts can last from a few seconds to many hours. (See tables 1–3 through 1–5 for blackout duration estimates.)

**Table 1–3. Blackout of High Frequency Communications System**

| Burst Region | Mode of Propagation | Blackout Source | Estimated Duration of Blackout |
|---|---|---|---|
| High altitude | High frequency, skywave | Ionized region | Minutes to many hours |
| Low altitude | | | |
| Near surface<br>Surface<br>Sub-surface | Skywave, groundwave, high frequency | Fireball | Negligible to few seconds |

*Source:* US Army Nuclear Agency, "Blackout of Tactical Communications," note no. 4, August 1976.

Blackout occurs when radio waves pass through a disturbed region causing a refraction or bending of the wave. Essentially, the transmitter sends a signal at a given frequency, but the wave bends and arrives at the receiver at a different frequency—the result is distortion or blackout.

Communications blackouts in front line units occur when the fireball or dust cloud created by a nuclear explosion interdicts radio transmission paths. These front line systems are called line of sight systems, and their blackout lapse time can range from a few seconds to a few minutes (table 1–4).

The high altitude bursts (see table 1–5) are the most significant for satellite communications blackout and HEMP. Blackouts could last for several hours, but unless satellites are hardened, HEMP could severely hamper or virtually wipe out satellite communications.

Wire communication does not rely on information passing through the atmosphere. As long as microwave links are not integrated into the wire communications net, wire remains unaffected by blackout. The prudent military planner, however,

**Table 1–4. Blackout of Line of Sight and Troposcatter Communication**

| Burst Region | Mode of Propagation | Frequency Bands | Blackout Source | Estimated Duration of Blackout |
|---|---|---|---|---|
| High altitude | Troposcatter | UHF, SHF | Scatter from Fireball | Few seconds to minutes |
| Low altitude<br>Near surface<br>Surface<br>Subsurface | Troposcatter | UHF | Dust/Fireball | Few seconds to tens of seconds |
| Low altitude | Line of sight | VHF, UHF, SHF | Fireball | Few seconds to tens of seconds |
| Near surface<br>Surface<br>Subsurface | Line of sight | SHF<br>UHF<br>VHF | Dust/Fireball | Few seconds to a few minutes |

*Source:* US Army Nuclear Agency, "Blackout of Tactical Communications," note no. 4, August 1976.

**Table 1–5. Blackout of Synchronous Satellite Relay Systems**

| Burst Region | Frequency Bands | Blackout Source | Estimated Duration of Blackout |
|---|---|---|---|
| High altitude | UHF, SHF | Ionized region | Few minutes to hours |
| Low altitude | UHF, SHF | Dust/Fireball | Few seconds to tens of seconds |
| Near surface<br>Surface<br>Subsurface | UHF, SHF | Dust/Fireball | Few seconds to tens of seconds |

*Source:* US Army Nuclear Agency, "Blackout of Tactical Communications," note no. 4, August 1976.

cannot rely solely on wire as a solution to communications in a nuclear conflict, because the wire serves as an antenna for HEMP. The equipment linked to wire (repeaters, digital switches, computers, etc.) will be subjected to voltage surge and burnout. Precautions against HEMP must be foremost in the planners' minds. In this regard, in Europe the German military has placed its communication lines underground. At predetermined locations, mobile communications units could tie into the German Army underground communications net, the Grundnetz. Unfortunately, the US Army is not yet tied in. If the US Army does tie into the Grundnetz, undoubtedly, it will be only for extremely high priority communications.

In Germany US Army long line communication links rely heavily on the national communications system, the Bundespost, a system which is similar to "Ma Bell." Unfortunately, this system is not underground and is extremely vulnerable to all types of enemy interdiction, ranging from sabotage to EMP. (Fixed installations in Germany, as in the United States, are highly susceptible to sabotage.) A US-NATO-German analysis of the entire European communications system, with the objective of communications survivability, is indicated because of this susceptibility. Some initiatives that would make the European or any theater communications system less vulnerable follow:

- Identify critical links and nodes and plan on protecting these vulnerable points in war with better physical security (fences, lights, towers, camouflage).
- Plan for using or constructing alternate nodes to critical links.
- Bury the Bundespost (long line) in a manner similar to the Grundnetz (tactical).
- Preposition end items and repair parts at critical locations.
- Connect the US to underground host country tactical systems.
- Equip more units with hardened shelters and make them more mobile.

Without reliable communications in war, information stored in the computers becomes degraded, untimely, and inaccurate. Thus, the Army should be aware of these shortcomings and plan accordingly for Europe and for all possible theaters of operations, including the continental United States.

## COMPUTER EQUIPMENT

In addition to the NBC environment, shelters, and communications links, the computer equipment itself requires attention. At the present time, there are deficiencies in the way our computer equipment is developed, procured, fielded, and maintained.

### PROCUREMENT

One of the first computers used in the theater of operations in the late 1950s was the "Moby Dick," a military specification computer. By our current standard, it was a monster—costly, slow, relatively immobile, and unreliable. By the late 1960s the majority of the military computers, excluding embedded computers, purchased for the theater of operations were the relatively cheap commercial computers packaged in a case, "ruggedized," and housed in a shelter (van).

The Army purchased commercial computers instead of military specification computers for three reasons. First, in 1965, Congress passed the Brooks Bill, a law designed to foster competitive procurement of automatic data processing equipment (ADPE). This law gave the House Government Operations Committee (GOC) congressional oversight over ADPE procurements. Using their newly acquired oversight authority, GOC strategy focused on reducing sole source procurements. These oversight pressures caused the services to move away from military specification computers and toward the purchase of the least expensive commercial computer.

Research and development (R&D) was costly in the highly competitive computer industry; consequently, R&D results were highly guarded and considered to be the proprietary right of the company that performed the R&D. Normally, unless R&D performed under Army contract has security implications, it becomes public domain—available to all computer com-

panies. Thus, to avoid possible legal difficulties, computer companies prefer to perform their own R&D.

To minimize individual company R&D expenditures, in the 1960s, computer companies began to market their newly acquired computer technology to the military. These commercial computer sales to the military were highly profitable to the computer industry and inexpensive to the military, especially when compared to the cost of military specification computers. As the DOD budgets got relatively smaller and commercial computers got cheaper, pressures from within DOD and from Congress virtually dictated that the Army buy commercial, general purpose computers.

In the last 10 years, computer companies have found it too cumbersome to abide by all of the Government procurement regulations. The industry continually expresses its displeasure in doing business with Government. Currently, private sector business is nine times the amount of Government business. And, with greater than 20 percent return on investment in the private sector market as compared to a return on investment of less than 10 percent from Government business, the computer industry now finds it less profitable to pursue Government business than it did from 1960 to 1973.[6] Individual computer companies are selling their commercial computers to the military to maintain volume sales, but computer companies are apt to balk at selling military specification computers to the Government if it will involve R&D expenditures and proprietary rights questions.

For example, the Army tried to obtain the proprietary rights for a 32-bit computer architecture from a computer company to standardize its theater command and control computers. The Army's request for proposal to build these 32-bit computers was essentially unanswered by the computer industry (one response). In pursuing the reason for the industries' nonresponsiveness, the Army was told by several of the computer companies that they chose not to bid because they feared a suit on subsequent developments of their commercial computers, based on the proprietary rights issue, by the original owners of the 32-bit architecture.

The underlying force in military computer procurements

has been fiscal constraints. As an example, to keep costs down, US companies and the military have demonstrated little concern about EMP. With the EMP threat minimized, yesterday's computers with their vacuum tubes and transistors could rightly ignore EMP. Today, the Army with its vulnerable integrated circuit computers cannot ignore EMP. Thus, our past effort to save dollars on commercial computers may end up being a double-edged sword, costing us valuable time, money, and effectiveness while we wait to develop new survivable computers or modify our old computers through difficult and expensive retrofit and redesign.

Incorporating these EMP design standards into military computers can be accomplished in three ways—by setting military specifications for military computer developments, by establishing minimum industry-Government standards for commercial computer developments similar to the Environmental Protection Agency standards for selective industries, or by a combination of the above two whereby commercial computer specifications are raised to satisfy military use.

The last approach may be preferable, but it won't be easy to convince industry. To go this route costs money. In this approach DOD or some other governmental agency would sponsor R&D for an EMP design effort, similar to DOD's very high speed integrated circuit (VHSIC) program. In one sense, the VHSIC program could be viewed as Government supported R&D from which the nine participating major computer companies expect to obtain a technology spinoff. During a second phase, the VHSIC program will reduce the participants to five companies. At the conclusion, the remaining participating computer companies should have an edge in very high speed circuit adaptation to the commercial market. Market shares could be gained in the process. The same rationale can be applied to an EMP R&D design effort. If it is lucrative, as in the VHSIC program, industry will compete to participate in the R&D effort.

This effort relates to defining military specifications for equipment development; in practice the military has tended to specify restrictive requirements which ultimately cause equipment to be overdesigned. Thus, attention must be directed toward identifying requirements, specifying minimum standards,

and allowing industry to develop the end product. In the EMP area, DOD must develop standards in penetrator protection and isolation, in shielding protection and in specifying telecommunication test standards.[7]

Today, a plethora of computers, such as IBM 360s, IBM 370s, Honeywell level 6s, Honeywell 6000 series, TI 99s, Apple computers, and Univac 1005s, comprise front-line equipment. Each computer requires differently trained repairmen and operators, a unique repair parts inventory, different operating procedures, and more operations and maintenance dollars to stay in operation. Undoubtedly, the number will grow, and the uses and problems will increase. What kinds and varieties of computers will dot the battlefield? By 1986, plans indicate that each brigade headquarters could have as many as three different and unique computers—one for logistics, one for operations, and one for intelligence. Current procurement practices could create battlefield chaos by 1986; thus, the need exists for standardizing these theater computers, such as under the military computer family.

## COMPUTER MAINTENANCE

Computer maintenance is a significant problem area when one or more of the following factors is missing—repair parts, repairmen, and backup computers.

*Repair Parts.* The more different computers there are to support, the more difficult it becomes to provide repair parts support. This difficulty becomes especially notable with standardization of computer repair parts virtually nonexistent among computer manufacturers. Each manufacturer has a unique product line with marketable attributes. In addition, the Army's practice of contracting with several manufacturers to provide repair parts can be costly and, in some cases, unreliable. If two computers made by different manufacturers are inoperative and the parts to repair the computers are not immediately available, the using unit cannot interchange parts between the inoperable computers to make one of the two operable (cannibalization). In war when supply lines are often severed and parts are in short supply, such cannibalization becomes, in many cases, the only way to maintain equipment.

There's also an age factor to consider. Active Army computers are an average age of about 9 years, and Reserve component computers average 13 years. So far, computer technology has been turning over every 2 to 4 years, and some computer manufacturers have stopped providing the repair parts for these obsolete computers after about 8 to 10 years. Computer parts become more expensive when contractor repair parts production lines are kept open only for the Army.

*Repairmen.* Army computer repairmen, another critical factor in the maintenance equation, are few. When it is time to reenlist, the repairmen are hired by the contractor who manufactures and sells computers to the Army or to the civilian market. Since the Army training cadre is small, the contractor provides the majority of our computer repairmen's training. (The training is tailored to the contractor's computer.) In Vietnam we relied on contractor maintenance, but Vietnam was not a nuclear war. There, computers existed only at well-protected base camps. And, even though Vietnam was a safe, profitable war for computer contractor repairmen and their companies, IBM computer repairmen tried to leave the country during the 1968 TET offensive.[8] Fortunately for Army, no commercial aircraft could land at Saigon's Tan Sonhut Airfield. Some argue that in any war, with enough money, contractor maintenance will not be a problem. Can we afford it if this hypothesis is wrong?

*Backup Computers.* In war what would happen if a computer or its shelter were destroyed? Neither the Army nor the contractor maintains end item stockage to replace the destroyed shelter or computer. In fact, if it is a relatively new computer, the contractor has many unfilled commercial back orders and no responsibility to replace destroyed Army computers. A replacement computer cannot be provided until the Army either takes one away from another active or reserve component unit or until the contractor, by readjusting priorities, finds a compatible computer, redirects a scheduled shipment from a customer, or produces another computer. If the computer requires repair work, its unit remains without a computer and must borrow computer time from a neighboring unit until the "deadlined" computer can be repaired or replaced.

Consider the numbers involved. A Department of the Army Readiness Command (DARCOM) Plans Review Committee identified 58 different computers supported by 24 manufacturers, 43 computer languages and 250 support systems scheduled for development and subsequent shipment to units.[9] Through the 1980s the General Accounting Office (GAO) contends "the Army, the Air Force, and the Navy estimate they will deploy 13,000, 40,000, and 33,000 computers respectively."[10] (Although not specified in this GAO report, many of these computers are integral parts of large weapons systems.)

An alternative to backup computer support is establishing a stock of loan computers—a regular occurrence in the Army. For example, if a radio or a computer is damaged but is repairable, a loan item (maintenance float) is issued to the unit requesting repair. After the damaged item is repaired, it becomes the float item. The end item density and the mean time to repair that piece of equipment determine the number of end items carried as float. With contractor computer maintenance in the theater, this maintenance float procedure does not exist in computer maintenance operations.

With current trends toward battlefield automation, placement of incompatible computers in the field is only the tip of the iceberg. Hidden beneath is a wide range of incompatibility problems—computer languages, terminals, peripherals, software support systems, architectures, buses, cables, etc. This proliferation of incompatible hardware and software is an impediment to interoperability, transportability, and, most importantly, survivability. Should this proliferation of computers, languages, and instruction-set architectures continue, technology upgrade will become impractical without rewriting expensive software.

In 1960, hardware represented 90 percent of the ADPE costs; today it represents 20 percent with 80 percent of the cost going to software development and software maintenance. By 1990, software costs will increase to about 90 percent of system costs. Should we continue on our present course, more and more software will be locked into a large number of instruction-set architectures housed in older hardware. System maintenance and readiness will decrease as

equipment becomes obsolete, repair parts become scarce, and qualified repairmen become invisible.

It follows that standardization is one effective way to head off the continuing proliferation of incompatible equipment. With computer standardization, the Army can conduct training, doctrine, and maintenance courses. Then, hardware procurements can produce compatible equipment programed in a standard language; logistics support policy can be efficiently developed and implemented; and flexibility, operability, and survivability will be enhanced while vulnerabilities are reduced.

## STANDARDIZATION

In an effort to resolve the computer procurement and maintenance problems, the Army has taken its first step to standardize Army computers—with the development of a military computer family (MCF). The MCF standardization initiatives are moving forward along three fronts—*hardware*, *software*, and *instruction-set architecture*.

*Hardware*. *Hardware* in the MCF will consist of three standard computers—a single module (card) computer, a microcomputer, and a superminicomputer—all designed to increase computer survivability in the field by stressing reliability and maintainability and by providing for computer redundancy and standardization. (See table 1-6 for each computer's capabilities.) Rather than fielding 58 different computers between 1986 and 1991, the developed MCF would field three computers to satisfy battlefield automated systems requirements. This is standardization to provide redundancy, three identical computers at brigade level to make backup compatible computer power available immediately in the event one computer is destroyed or fails to operate. Current procedures require backup support to be provided by the corps or the adjacent division's computers—computers that are overworked and not easily accessible. MCF would drastically reduce these problems in operations continuity.

Experience has also shown combat commanders that controlled cannibalization and parts interchangeability can mean the difference between funtional and nonfunctional

**Table 1-6. Military Computer Family Development Goals**

| | Super-Minicomputer | Micro-computer | Single Module (Card) Computer |
|---|---|---|---|
| Performance | 3 MIPS | 500 KIPS | 500 KIPS |
| Memory | 2M bytes | 1M bytes | 128K bytes |
| Size | 0.5 $ft.^3$ | 0.1 $ft.^3$ | 6 by 9 by 1/2 in. |
| Weight | 40 lb. | 10 lb. | 3/4 lb. |
| Power | 100 watts | 20 watts | 5 watts |
| Reliability | 10,000 hr. (MTBF) | 33,000 hr. (MTBF) | 100,000 hr. (MTBF) |
| Virtual address space | $10^9$ bytes | $10^9$ bytes | $10^9$ bytes |
| Maintainability | 30 min. (MTTR) | 15 min. (MTTR) | Remove and replace |

equipment on the battlefield. With the MCF, once the computers are standardized, so that computer and item densities are large enough to support logistics stockage and float policies, training and maintenance doctrine and manuals can be developed and military repairmen can be trained and assigned to theater units.

Another MCF factor that enhances computer survivability on the battlefield is standardization of computer weights and sizes. The weights and memory sizes of the three MCF computers are smaller, ranging from three-fourths of a pound to 40 pounds and from 128,000 bytes to 2 million bytes. In turn, serious consideration should be given to reducing the size of the shelters that house computers. Reduction of the current "18 wheeler" vehicle-shelter combination to a 2½-ton 109 van or a smaller vehicle/van combination could drastically reduce computer installation silhouettes, making camouflage easier and enemy detection more difficult.

In addition to the above, the Army needs to simplify the procurement process for obtaining theater-level, mission-critical computers. Currently, there are two separate procurement regulations for buying field computers to be located within 10 to 15 miles of the forward edge of the battle area: a regulation for logistic and administrative computers, Army Regulation (AR) 18-1, and a regulation for embedded and command and control computers, AR 1000-1. These two different regulations are required by the Brooks Bill (Public Law (PL) 89-306) and the Paper Work Reduction Act (PL 96-511). Even the wording of the 1982 Defense Authorization Act (PL

97–86) doesn't alleviate the requirement for two regulations. However, it is anticipated that DOD interpretation of PL 97–86 will play a major role in solving the computer compatibility problems in the theater. For example, how will DOD and Congress view a computer that keeps track of ammunition in a division—is it an inventory/stock control computer or a critical computer for the direct fulfillment of a military mission? The distinctive essential elements of PL 97–86 follow:[11]

*Excluded* from the Brooks Bill, ADP procurements of computers for

- Intelligence activities
- Cryptologic activities related to national security
- Command and control of military forces
- Weapons or weapons systems
- The direct fulfillment of military or intelligence mission

*Not excluded* from the Brooks Bill, ADP procurements for the

- Military and civilian pay system
- Financial management system
- Stock control, storage depot and base level system
- Military and civilian personnel management systems
- Medical management systems
- Civil works system
- Office automation system

Law interpretation relates here, because during war, theater logistics and personnel systems are not just accounting systems. They are also mission critical command and control systems with major operational impacts. Supply shortages in petroleum, ammunition, and barrier materials can alter an entire battle or change a preferred course of action. Worse yet, not having knowledge of the shortage condition could result in the loss of a company or platoon.

It follows that expansion of the MCF beyond its initial command and control boundaries, to encompass all theater mission critical computers, would eliminate the need for two separate procurement regulations. Therefore, action should be taken to identify *all* field computers as mission critical com-

puters under the procurement policies of AR 1000–1. At a minimum, the Army needs MCF computers used throughout the theater, with procurements for battlefield computers excluded from the Brooks Bill (if the Army type-classifies the MCF computers as the standard theater computers). The MCF should save the Army money, time, and the frustration associated with buying computers. In fact, the initial cost benefit analysis shows a $34 million cumulative savings by 1985 and over $1 billion savings by 1993.[12]

*Software*. Software standardization requires one computer language and a standard computer language compiler. DOD approved Ada, a high-order programing language, on 1 January 1981 as the standard DOD language. So, from 1 January 1983 all battlefield automated systems under engineering development, less administrative and logistics systems, are required to use the Ada language. Currently, MCF is designed for only one compiler, Ada. Since logistics and personnel systems are written in COBOL, they cannot use MCF computers unless (1) logistics and personnel systems are rewritten in Ada, or (2) a translator is built to convert COBOL to Ada, or (3) a COBOL compiler is built for the MCF. A time-phased plan to evaluate these three alternatives is required before MCF development is too far along (approximately 1983). In the event that the third alternative (build a COBOL compiler) is selected, the COBOL compiler should be built before the MCF production decision is made.

Generally, programing languages neither cause nor solve software problems, however, because of their central role in software development, languages can either aggravate existing problems or simplify their solution. As a high-order language, Ada provides some definite advantages over other languages:

- Enhanced transportability, the ability of the program to be used on other systems.

- Enhanced real time interactive processing.

- Standard documentation and a communication medium among different battlefield automated systems and between the systems engineer and the programer.

- Standard training with little need to cross-train in other programing languages.

- The basis for a reduced software problem and a reduction in life cycle costs.

There are also major disadvantages. Ada is a more complicated language for the programer to learn, and Ada does not provide as many convenient built-in features for data formatting and input-output processing. With increased use, we will be able to tell if Ada's advantages outweigh its disadvantages.

Increased programer productivity would strengthen the Federal Government's position in managing its scarce computer programing resource. This is significant, since Ada will increase programer productivity, and computer programer availability is expected to become more critical during the next 5 years. From 1979 to 1984, US minicomputer production will more than double to 382,000 units per year.[13] Parallel to this demand for computers will be a demand for programers. At present, Government programer salaries are not comparable to those in industry, and in addition, the computer programer market is not keeping pace with programer requirements. Should these conditions continue, as long as commercial computers are in the field the Army will continue to lose programers. Computer programer shortfalls are continuing to develop—read the want ads in Sunday's paper. Standardization of programing languages (along with the computer instruction-set architecture) serves as a partial solution to our slumbering computer programer problems. However, this sleeping giant could awake and cause slippages in timetables for providing computers to the field.

*Instruction-Set Architecture.* The controversial aspect of the MCF program is the standardization of the *instruction-set architecture*. The General Accounting Office's and industry's major argument against this standardization is that it will stifle and delay the contractors' use of state of the art technology; hardware and architecture standardization will automatically place the fielded MCF—even with a planned technology insertion program—one generation behind technology advancement. The MCF time-phase plan calls for a new upgraded

MCF every 5 years. With computer technology turning over every 2 to 4 years, this means MCF will be nearly 8 years old before it is replaced with an upgraded MCF. So, what's new? Today's division combat service support and theater command and control computers are without a standard instruction-set architecture, have different operating systems and computers, and are well over 10 years old. At least, with standard instruction-set architecture in the MCF, software changes will be minimal.

Under current procedures, each battlefield system manager or contractor has to develop a unique operating system for each computer series purchased. Operating system software, the most difficult and expensive software to develop, is hardware and software contractor dependent. This approach individualizes development, increases cost and risk, and aggravates the problem of post-development software support for battlefield systems. Thus, each system fielded has its own software and hardware uniqueness—and we have an octopus out of control.

Instruction-set architecture, on the other hand, should ensure that the operating system, Ada compilers, memory interrupt, input/output, and central processor instruction sets are the same among MCF production line manufacturers. With MCF processors, architecture, and Ada-based common software tools, the program manager can provide the contractor with well defined requirements and direction, instead of reacting to questions on technical hardware and software specifics regarding systems development. At the center of the MCF standardization process is the simplicity that is obtained by keeping changes and complexity away from the field environment.

## DISTRIBUTIVE PROCESSING

In addition to simplicity, standardization provides flexibility. The three standard compatible MCF computers give the Army just that. A distributive system, once developed, could provide an option which decentralizes management functions, computer processing, and computer operations. Such systems increase survivability during war by providing the user with flexibility through equipment and system redundancy and

through the decentralization of functions. Significantly, trends in the commercial industry have shifted from large centralized systems, controlled and operated by data processing personnel, to smaller distributed systems, controlled and in many cases operated by the functional user. The Army, too, must begin the evolutionary path which treats the computer and its information as a tool—a resource that the functional manager can use efficiently to achieve mission objectives. Distributive systems with MCF initiatives should increase survivability, ensure continuity of operations and dispersion on the battlefield, and provide flexibility through redundancy during periods of partial incapacitation or equipment relocation.

# 2. THE WHOLE IS GREATER THAN THE SUM OF ITS PARTS

What, then, are the implications for command and control systems? Insights can be drawn from (1) review of the Russian threat and doctrine which specifically target US command and control systems, (2) examination of the level of integration of the functional components into an integrated command and control system, and (3) identification of the support requirements for command and control systems.

## THE THREAT

Soviet doctrine for radio electronic combat specifically targets US command, control, and communications ($C^3$) systems.[1] This is significant, since the Soviet Army is a well organized enemy, equipped with modern weapons—more mobile, more numerous, as lethal, and better protected by electronic countermeasures—to take advantage of a disorganized foe with ineffective command and control. What we face in the Soviet Army is not only superior in most significant military numbers, it is also superior in the application of automated technology for controlling those forces for combat.[2]

It is an irony that the leader in technology, the United States, is behind the Soviets in computer assisted command and control systems. According to Soviet military writers and US intelligence evaluation of the Warsaw Pact's field exercises, the Soviets are at least 5 years ahead of the United States in using computers for command and control.[3]

One of the first Russian computers, the Ryiad, looked much like the IBM 360 computer series, a computer of the late 1960s. At present, although Soviet computers are clearly behind US computers, the Soviets have taken a simplistic ap-

proach which provides them flexibility through standardization of the computers in their command and control system. Their computers are compatible, permitting easy integration of command and control systems in times of crisis. Unfortunately, in the face of this Soviet standardization, no provision exists for interoperability of automated systems within the NATO forces.[4]

## THE COMMAND AND CONTROL SYSTEMS

US command and control system developments have been piecemeal, with little central direction for integration of functional systems. At the division and corps levels, US integrated battlefield command and control systems obtain key elements of information from five functional systems—maneuver control, fire support, air defense, intelligence and electronic warfare, and combat service support. All are tied together by a vital communications network and referred to as the SIGMA system (illustrated at figure 2–1).

Each functional system has a command and control system of its own. The differences between this functional system and the integrated command and control systems are the levels of detail of the information collected, processed, and used to control military forces and operations. The functional systems must be able to respond to requirements originating from the integrated corps or division level system. Since the integrated and functional command and control systems are interrelated, the development of each system will impact significantly on the results obtained from any of the other systems. To ensure compatibility among command and control systems, someone should carefully orchestrate each system's development.

## FUNCTIONAL SYSTEM DEVELOPMENT

To completely grasp the philosophy that has been prevalent behind functional system development, the following overview of one functional system, the maneuver control system, is helpful. (The maneuver control element is under the direct control of the operations officer (G–3) of a brigade, division, or corps. This officer is also the integrator of command and control on the battlefield. Thus, the integrated com-

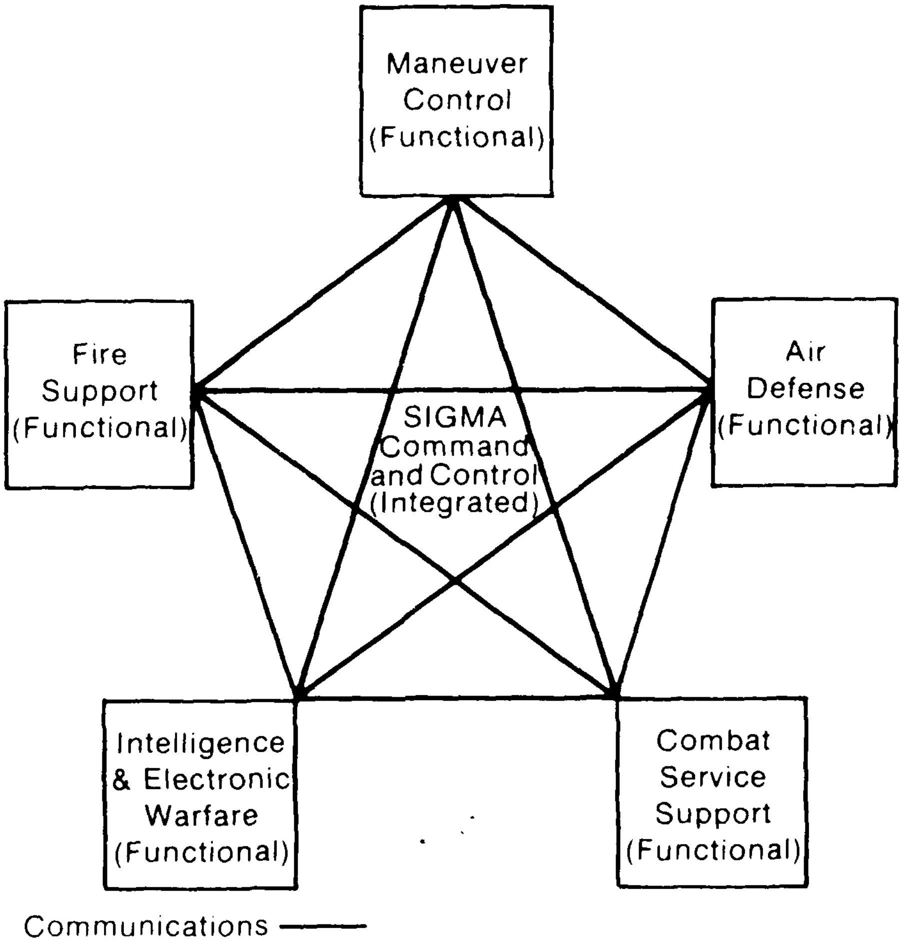
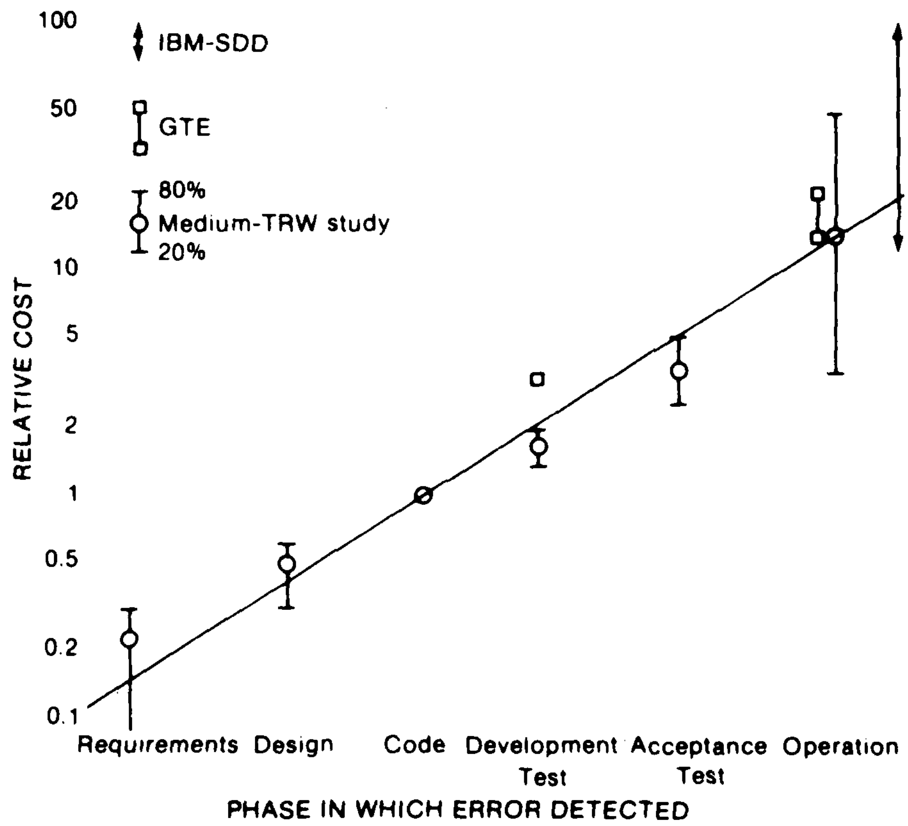



**Figure 2-1. The Battlefield Automated Command and Control Network**

mand and control system and the maneuver control system are co-located at each level of command.)

The maneuver control system was designed for command and control of the maneuver element of the force from the echelons of corps through battalion. Its primary emphasis is on handling battlefield information reporting, friendly situation data, operations orders, and unit task organizations.[5] Its development and design (phase one) uses a bottoms up approach. This includes user involvement and testing to ensure real world validation of requirements and the stabilization of the baseline before adding additional increments to the baseline system.[6] In actuality, each functional system uses this bottoms up development approach.

The second phase of the maneuver control system will be an evolutionary outgrowth. It will provide a full data base storage and retrieval capability, as well as decision support functions, and will include the integration of command and control functional systems into an integrated SIGMA command and control system. During the integration processing of the five separately designed systems, problems will surface. (Each functional system is expected to provide compatible data for use by the integrated command and control system.) Experience has shown that the integration of subsystems is the most critical period in the bottoms up system development approach. It costs less to make changes early in the system development process (figure 2–2). Making a change in the oper-




*Source:* Barry Beohm, "Software Engineering," *IEEE*, C–25, (December 1976).

**Figure 2–2. Relative Cost to Fix an Error During System Development**

ations and development phases of a system is 100 times and 10 times more expensive, respectively, than making a change in the requirements phase of systems development.[7]

### INTEGRATING FUNCTIONAL INFORMATION

As of March 1982, requirements for the integrated command and control system had not been published, yet each functional system continues its development trek to eternity. Action should be initiated to define the requirements for the integrated command and control system before the functional systems are totally developed; otherwise, we may discover that integration may be impossible without major functional system revisions. The Army should refine and revise its development of the integrated command and control system from its bottom up approach to a top down development approach.

With a top down approach to the SIGMA system, the data flow for the functional system must be finished and the information requirements for the integrated system identified. Then, development can start by producing a crude skeleton version of the system. Once the skeleton version of the integrated system is working on real machines, then complexity can be added to the functional systems for evolutionary development.[8] Evolutionary development of the functional systems will ensure user acceptance of the system and ensure information required to perform the user's mission is, in fact, provided by the system.

### INFORMATION WHERE IT'S NEEDED

Integrating the functional command and control system into the SIGMA force level command and control system connotes centralization—the bringing together of decentralized elements. Such centralization tends to grow geometrically, if unchecked, into a large command post configuration. The Army should avoid large centralized command posts. Instead, it should develop mobile cells which can be dispersed and easily concealed from the enemy, visually as well as electronically; these cells can represent the functional command and control system at each level of command.

Integration of the information contained in these dispersed cells can be accomplished with distributed computer

processing interconnected with communications. In the division, the functional cells responsible for providing SIGMA force level requirements at each level of command, down to brigade level, should have the same capability as the division control cell. (The division control cell is responsible for providing the integrated data from the functional system into the SIGMA force level system for the commander.) This capability is necessary for the following reasons:

- The division or corps commander is seldom always at the main command post. If the commander is forward, force level command and control information can be obtained from the brigade level command posts. Without this dispersed command and control capability the commander would either lose command and control of the corps/division when forward or remain tied to the main command post.

- Under Division 86, the brigade has the capability to function as an autonomous unit; if the division main command post is inoperable, the brigade commander/brigade command post can act as the command and control center for the division.

- With each command post possessing current information, system redundancy is guaranteed, and each commander can get an identical snapshot of the battlefield.

To effectively implement the SIGMA force level command and control system, the Army should move toward distributive data processing systems. In such systems the key element is networking and communication links. Also a critical element in an effective automated command and control system is the integration of functional systems at the command post level. If missing one of the critical elements, the command and control system is inefficient, untimely, and ineffective. Currently, if in fluid wartime conditions, communication is by FM radio or courier. In the future, communications systems will also include the Position Location Reporting System for low volume transmissions and the Joint Tactical Information Distribution System for high volume transmissions.

## DEVELOPMENT RESPONSIBILITIES

Responsibility for the development of battlefield auto-

mated systems rests with three commands—Training and Doctrine Command (TRADOC), Materiel Development and Readiness Command (DARCOM), and the Computer Systems Command (CSC) (figure 2–3). User requirements for all battlefield automated systems are formulated and documented by TRADOC.

Requirements for system design and development for battlefield systems are split between DARCOM and CSC. DARCOM, with the project manager, assumes total responsibility for development and fielding of all battlefield automated systems, sans the combat service support system which is CSC's responsibility to develop and field. This split responsibility for providing support to battlefield automated systems adds complexity to the already difficult task of simplifying and making battlefield systems compatible for the following reasons:

- Hardware and software responsibilities are shared by two different supporting commands.

- Acquisition strategies are in conflict. (DARCOM is moving toward a military standard survivable system, and CSC toward a commercial "ruggedized" system with questionable survivability.)

- Undue regulatory conflict exists between AR 18–1 and AR 1000–1.

- Logistics and personnel inefficiencies will not be recognized through hardware and software standardization, maintenance, and inventory and procurement procedures.

- Interoperability and communications become more complicated when dealing with different systems and development organizations.

As a solution for ensuring battlefield systems compatibility, we could assign CSC project managers responsible for developing theater level systems to DARCOM (figure 2–4).

Within DARCOM headquarters, the Battlefield Automated Systems Office coordinates the development of battlefield automated systems. (DARCOM noted that this office was too small to accomplish its task in the DARCOM-initiated Automa-

tion Commodity Command Study.[9]) There are other options. An alternative to an automation commodity command could be a directorate at DARCOM with a general officer, in charge of tying together battlefield automated systems development and fielding plans.

## OPERATIONAL SUPPORT RESPONSIBILITIES

After the battlefield systems are fielded, they must continue to receive some level of support from the combat developer (TRADOC) and the system designer (CSC or DARCOM). Requirements and systems have to be compatible for the 59 different computers from 29 manufacturers with 44 computer high order and assembly languages and 53 different support organizations. To ensure compatibility, the Army reorganized computer systems support along functional lines into 11 post-deployment software support centers. Two centers are under CSC and nine are under DARCOM.[10]

Once the systems are fielded, each post-deployment software support center will have an oversea team or a team designated for travel, to assist the user when needed. This user assistance will be required often. In peace, Army command and control systems are designed to undergo evolutionary development. In war, systems will periodically falter when stress-tested beyond any normal predeployment simulated war testing. Foreseeable resource efficiencies and force flexibilities could be achieved if each theater computer system used the same computer and the same computer language. Resources could be shifted to resolve problems in critical functions to balance the survivability equation. Clearly, the advantages of standardization also apply to command and control systems.

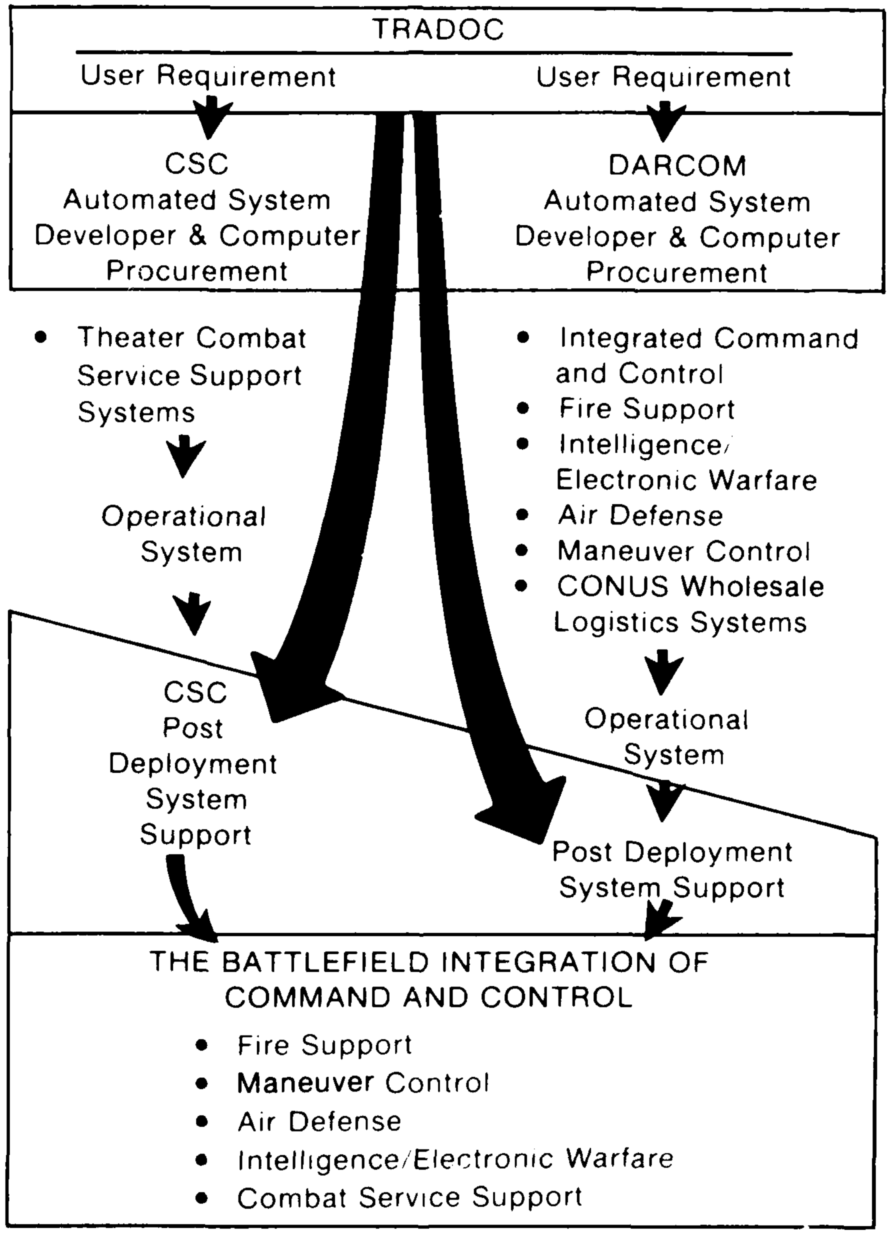



**Figure 2-3. Current Battlefield Automated Systems Development and Operations Support**

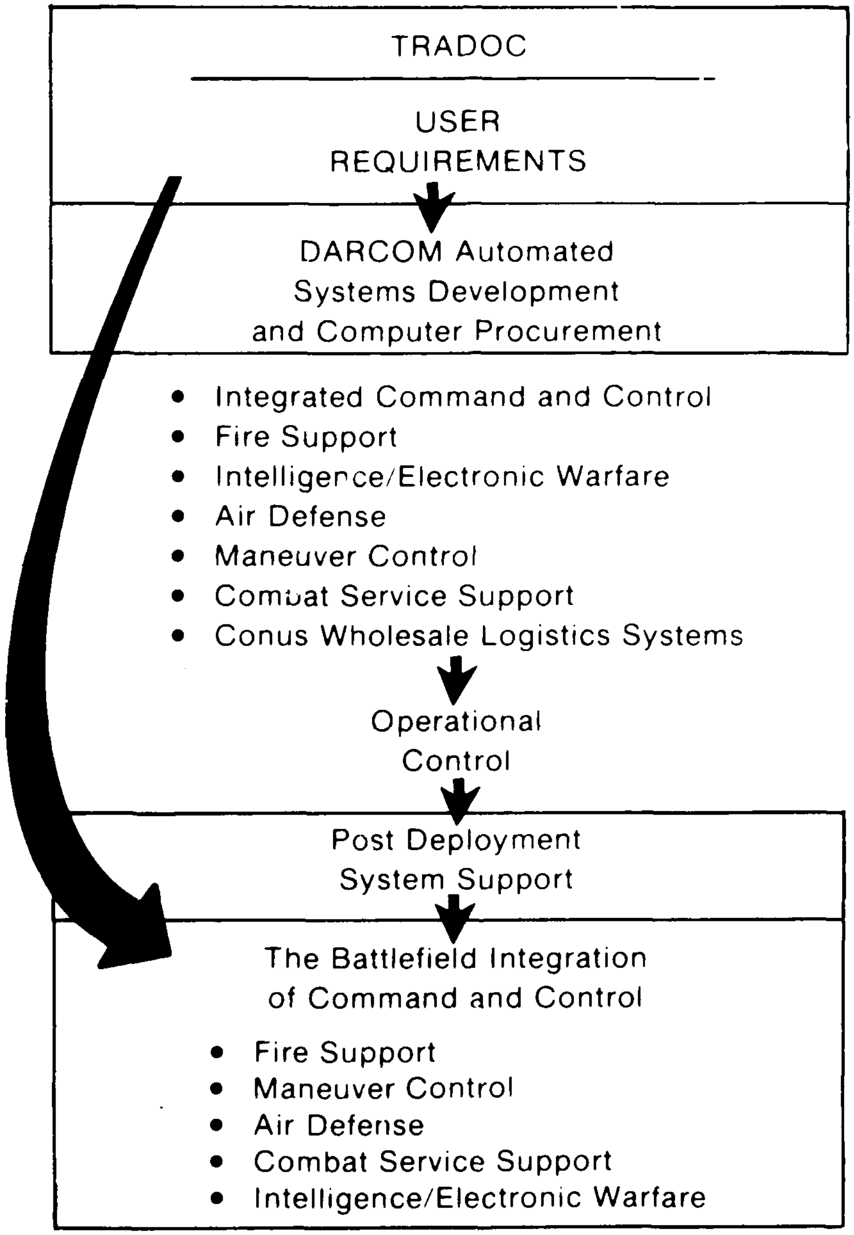



**Figure 2-4. Proposed Battlefield Automated Systems Development and Operations Support**

# 3. LESSONS LEARNED

Command and control system developments at the tactical theater level are in their infancy. Thus, we can take advantage of the lessons learned from the development of our more mature systems. For example, the supply system (appendix) is applicable to command and control systems. Its critical elements of reliability and availability are also key objectives of any command and control system.

Comments following in this section focus on factors which not only increase system survivability, but also increase system effectiveness. The discussions on functional and integrated command and control systems more fully explain the practical wisdom of the lessons learned in the supply system case in point (appendix). Other problem areas, personnel, training, maintenance, and standardization, are universal and applicable to other Army automated systems.

## PERSONNEL

Two personnel areas—assignments and authorization—identified as troublesome to the supply system are also applicable to command and control systems. The specific lessons learned follow:

- Don't delete spaces when converting manual to automated operations without considering the possibility of reverting to the manual mode in war.
- Consider using TOE automation augmentation for war.
- Be prepared to use and adjust the reenlistment bonus for critical computer skills.
- Consider establishing contractor dependent spaces as mobilization designee positions.

*Assignments.* As reviewed earlier, once the maneuver control and SIGMA systems are in the hands of troop units, the operations officer becomes responsible for the successful operation of the systems. These officers are essentially infantry officers. In 1982, about 767 or 6.5 percent of them had alternate ADP military occupational specialties (MOS). These ADP qualified infantry officers are assigned to data processing jobs which can be filled by any officer qualified in ADP.

The Movement Control System (MCS) will eventually be fielded in approximately 250 units. At a minimum MCS will be located at each corps, division, brigade, and battalion command post. The exact number of MCS units will depend upon the Army force structure. Each of the 250 MCS units should have an ADP qualified functional officer (infantry officer) in charge of operating MCS. With ADP becoming a tool of the functional manager, this person must be able to identify and use each of his or her ADP trained personnel.

Under the Officer Personnel Management System, the ADP officer assignment responsibility is rotated on successive tours between the functional manager and the ADP specialty manager. With the programed proliferation of ADP across all functional specialties, the requirement for ADP officers will increase drastically. To ensure utilization of functionally qualified ADP officers, the ADP specialty program should be dissolved, and assignment responsibilities should revert to each functional manager at the Military Personnel Center.

*Authorizations.* The Army concept of dispersing command posts into cells relies heavily on communications facilities transmitting information from one cell to another cell. Figure 3–1 depicts graphically the communications for the late 1980s that will be located on the battlefield from corps to company size units. A breakdown of any of the nodes in the communications network shown in figure 3–1 will cause an information imbalance in the system. Because of this possibility a backup system to balance the information flow is needed. A courier can serve as the backup means of delivering information from cell to cell. However, these couriers should not be functional personnel with designated missions. Instead, wartime courier augmentations to unit tables of organization and equipment (TOEs) should be established for each command post.

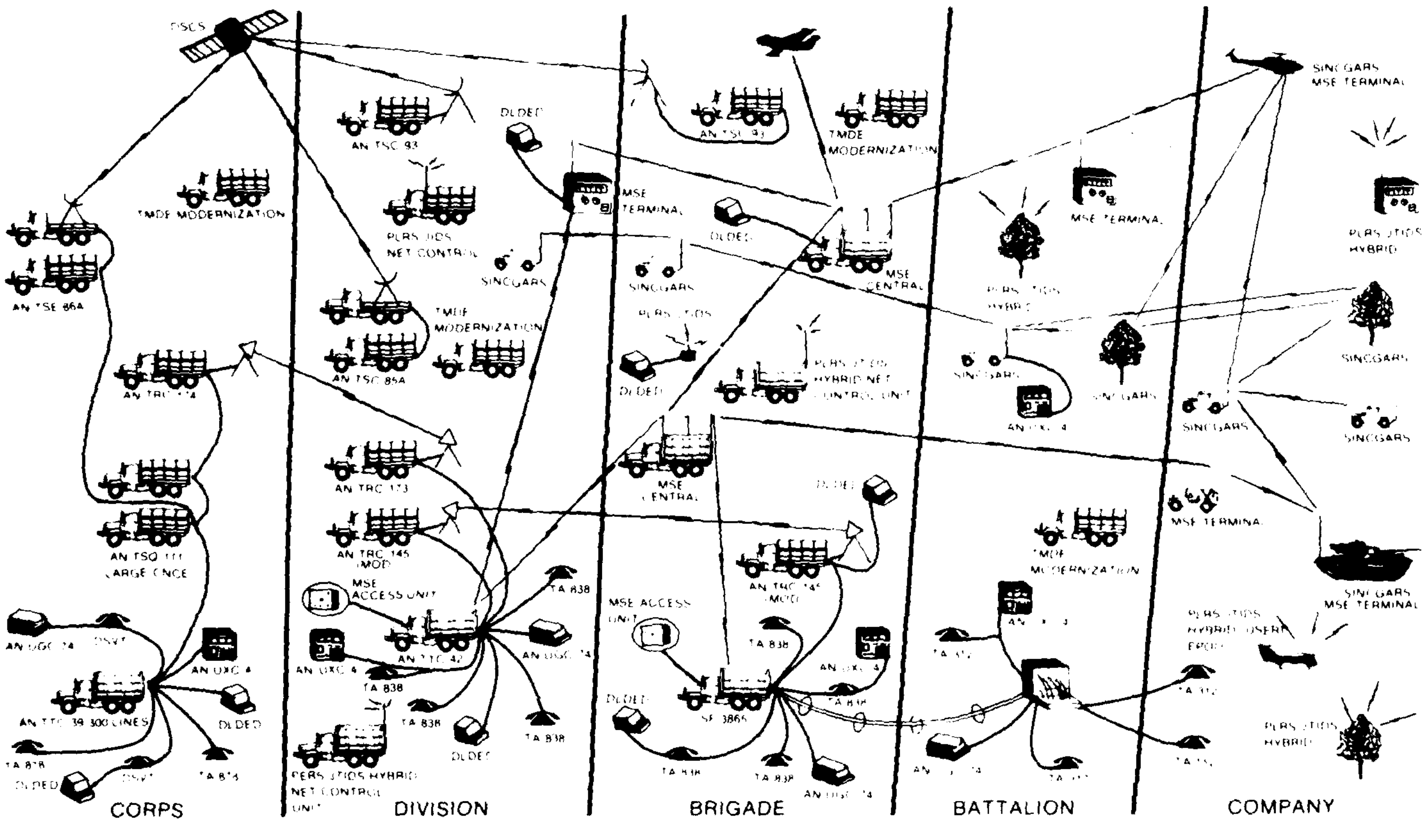



Figure 3-1. Battlefield Communications in the Late 1980s

Equipment and systems illustrated:

- ANTSC–86A. Satellite Terminal
- ANTSQ–111. Large (CNCE)—Tactical communication central facility
- ANTRC–174. Multichannel Repeater
- ANTRC 3. Multichannel Terminal
- ANTRC 145 (MOD). Multichannel Terminal
- ANUXC–4. Tactical Digital Facsimile
- ANTTC 39. Automatic Telephone Message Switching Central
- ANUGC–74. Automatic Communications Terminal
- TA 878. Telephone
- TA 838. Telephone
- DSVT. Digital Secure Voice Terminal
- TTC42. *Digital Nonsecure* Voice Terminal
- MSE Terminal. Mobile Subscriber Equipment
- SINCGARS. Single Channel Ground & Airborne Radio System
- TSC 93. Satellite Terminal
- TMDE. Test Measurement Diagnostic Equipment
- SB 3865. Automatic Switchboard
- SB 22. Field Switchboard
- *DCSC III. Defense Satellite* Communications System
- PLRS. Position Location Reporting System
- JTIDS. Joint Tactical Information Distribution System

**Figure 3–1. Battlefield Communications in the Late 1980s**—*Continued*

Authorizations can also be affected when highly manual intensive systems (such as the Intelligence and Electronic System) are automated; pressure will develop to give up the personnel (authorized for those positions) whose functions are automated. This pressure should be resisted until the system is fielded, operationally tested, and has undergone some evolutionary development. Unit authorizations or wartime augmentations must be retained for manual operations until our systems are made totally survivable.

*Training.* As of 1 April 1982, infantry officers received no ADP training at the Infantry School at Ft. Benning, Ga. (A special course for officers to be assigned to the maneuver control system should be established.) With more and more infantry officers coming into contact with ADP output and terminology, ADP training must be incorporated into the Infantry officer advanced course. Once again the training lessons learned in the case in point (appendix) are also applicable to command and control systems:

- Modify TOEs to reflect the specialized ADP skills required by the functional officer and require personnel requisitions to specify the training additional skill indicator for the job.

- Establish specialized ADP functional courses and assign an additional skill indicator to the graduates' MOSs.

- Ensure manual training is continued once the system is automated.

*Reserve Component Units.* With the exception of Combat Service Support, Reserve Component (RC) units have no ADP to support their command and control units at the corps and division levels. Thus, functional system automation plans must include the RC, and a decision to extend command and control systems to the RC must be considered soon. It appears better to maintain the RC in a manual mode than to create equipment and procedural disparities and incompatibilities between the RC and Active forces. If there is a decision to automate the RC systems, the training and personnel systems recommendations provided for in the appendix are applicable to command and control systems:

• Establish full-time technicians in RC units for their critical skills.

• Develop a contractor/college/Army program of instruction to train RC personnel.

• Establish a Sister Unit concept for training with the Active forces.

## MAINTENANCE

Even though the maintenance concept should be modular replacement with component repair to the rear or in the continental United States, closer to the forward edge of the battle area there is greater need for uniformed personnel to perform operator and minor direct support maintenance. Considering the number of new systems under development (and with standardization of computers as an Army objective), the number of computers on the battlefield will increase dramatically. Direct support repair capability will be needed in the theater. Certain repair and cannibalization functions will remain beyond the capability of operator maintenance and will be more cost efficient and force effective performed in-country.

## STANDARDIZATION

The need for flexibility is paramount in the command and control arena. Hardware redundancy and software transportability through standardization provide an inherent flexibility to command and control systems. Standard (MCF) computers would allow for the reallocation of computer resources to the most critical function in the corps, division, or brigade without the fears that follow:

• Equipment is not EMP survivable and is not mobile.
• Software is incompatible with the operating systems.
• Computer and the repair parts are obsolete or incompatible.
• Computer is not secure (Tempest tested).
• Programers and maintenance support personnel are not familiar with the hardware or software.

In addition, an objective in MCF design is to ensure that the future upgraded MCF is hardware and software compatible with the system currently being used by troop units. Subsequently, system fielding incompatibilities should be minimized.

PRECEDING PAGE BLANK-NOT FILMED

# 4. CONCLUSIONS: WHAT IS TO BE DONE?

Over the years our nation's defense has moved forward with technology—from the single-shot Kentucky long rifle to automatic weapons, from horse-drawn cannons to self-propelled howitzers, and from Marconi's wireless telegraph to space satellites. Electronic technology—computers, microprocessors, and integrated circuits—represents another breakthrough. Wise use of this technology can enable the United States to make decisions faster and more accurately.

Like many new technologies, microcircuitry provides great opportunities for use in defense systems. At the same time, however, it introduces problems that must be solved as nations and their adversaries expand the use of electronics on the battlefield. Computers now create problems in war. The challenge is to make computers survivable, inexpensive, reliable, and maintainable on the battlefield. Computers, once modified and fine-tuned, can hone our forces for a decisive victory.

What's to be done? Seven issues and specific recommendations for each issue are identified; implemented together they make computer systems survivable and reliable—an aid, not a problem, in combat.

*Issue 1: Fragmented Direction.* Fragmented direction exists at the Department of Defense and the Department of the Army for the procurement and development of theater automated computer systems.

To remedy the situation, the *Secretary of Defense* should

• Appoint either the Assistant Secretary (Comptroller) or the Under Secretary of Defense Research and Engineering as the DOD single point of contact for the military services on

military computer systems related to battlefield operations. One approval authority means one regulation for the services.

• Change the identifying names of the computers used to support soldiers on the battlefield from *embedded, command and control,* and *logistics* to *mission critical* and *nonmission critical* computers.

• Initiate action to convince Congress that all computers in the hands of soldiers at division, corps, and theater Army level are mission critical computers, including logistics computers.

Also in response to fragmented direction, the *Secretary of the Army* should

• Appoint a single command (DARCOM) to be responsible for the development of all mission critical computer systems (including tactical information systems being developed by the Computer Systems Command).

*Issue 2: NBC Survival.* Army computers, communications, and power sources currently fielded or planned for proliferation over the next 5 years are not NBC survivable.

With respect to NBC survivability, the *Department of Defense* should

• Establish two R&D financed programs similar to the VHSIC program—one on reducing the effects of EMP on electronics and the other on developing methods for decontaminating electronics in a chemical and biological environment.

• Inform Congress of the devastating effects that HEMP could have on electronics and communications in the United States. Use the results of its EMP research effort to convince the Department of Commerce to establish minimum EMP resistant regulatory standards on electronics produced in this country.

The *Department of the Army* should

• Establish a regulatory policy regarding the chemical survivability of computers and other electronic equipment.

• Develop modified chemical collective protection equipment with power sources compatible with the shelters and the vehicular power sources.

• Develop a lightweight chemical protective battle dress that enables the computer operators to better perform their mission.

• Ensure commercial computers (such as Apple or Sycor) used in the field are not performing functions which would be required during combat.

• Ensure adequate personnel are assigned or authorized as wartime augmentation to units operating automated systems, so that personnel are available for manual operations.

• Identify critical links and modes in theater communications systems and plan on protecting and developing alternative modes to critical links and alternative ways to communicate (such as by courier).

*Issue 3: Compatibility.* Army computers and computer systems on the battlefield are not compatible; this is causing ineffective use of resources.

The *Department of Defense* should

• Publish DOD regulation, 5000.XX–R, *Standardization Set Architectures for Embedded Computers*, and change the title to *Standardization Set Architectures for Mission Critical Computers.*

• Support the funding requirements for the Army's complete military computer family program.

With respect to compatibility, the *Department of the Army* should

• Provide funding for and expedite the completion of the MCF program—equipment, Ada language, and instruction-set architecture.

• Initiate a study to determine to what degree COBOL programs should be converted to Ada and develop a COBOL compiler before the MCF production decision is made.

• Extend MCF to all mission critical computers, not just battlefield automated systems.

• Require project managers to consider the total system for compatibility during the development process—the computer hardware and software, the shelter, the vehicle to transport the shelter, and all external power sources.

• Include the RC early in automated system development proliferation and upgrade plans.

• Emphasize the integration of functional systems in the command and control arena.

• Review NATO standardization requirements—a void exists on ADP equipment; move toward NATO/US development of Ada and MCF.

*Issue 4: Personnel Assignment.* Assignment policies do not ensure that trained ADP personnel are used in the positions for which they were trained.

The *Department of the Army* should

• Eliminate centralized management of the 53 specialty career field and allocate ADP position requirements to major functional specialties for management.

• Require functional experts to control ADP assignments using the primary and alternate specialties and, where applicable, by special qualification with an additional skill identifier.

• Require TOE ADP position requirements to be identified by primary and alternate specialty, and additional skill identifier, where necessary.

• Require field requisitions to use the entire individual qualification field (nine digits for officers and six digits for enlisted).

*Issue 5: ADP Training.* Programs of instruction of ADP functional courses for Active and Reserve component forces provide inadequate ADP training.

To remedy inadequacies, the *Department of the Army* should

• Establish a minimum number of hours of ADP training in

functional advanced courses, because ADP is becoming a management tool under the direct control of the functional managers; e.g., the Infantry School provides no ADP training in its advanced course.

• Include in special courses which produce functional ADP managers (such as DAS3) specific instruction on ADP security, continuity of operations training, and procedures for modifying systems software.

• Add a supply management course for field grade officers at Fort Lee. The course should emphasize management instead of the mechanics of computer data input needed to produce specific reports.

• Establish a tuition free program with community colleges and contractors to train RC personnel in ADP. Military service schools could then provide instruction on the adaptation of the ADP to specific military functional ADP systems.

• Establish the sister unit training concept for functional units with ADP systems such as nondivisional direct support units.

*Issue 6: Peacetime Operations.* Current peacetime automated systems are too cumbersome for wartime operations.

The *Department of the Army* should instruct TRADOC and functional system designers to

• Develop abbreviated wartime files from the current peacetime system for immediate implementation upon the outbreak of hostilities. Remove nonessential processing to the theater rear or the continental United States, e.g., financial management, demand analysis, and reduce status and followup processing in the theater.

• Incorporate into the centralized automated system the capability to decentralize operations to a lower echelon. For example, centralized automated supply systems at theater level should have a capability to decentralize receipt, issue, and storage processing to the operating battalions.

• Focus future systems developments around distributive processing with an interactive and batch processing capability.

*Issue 7: Computer Resources.* The lack of critical computer resources (programers, repairmen, computer end items, and repair parts) will cause a degradation in computer operations in a conventional war.

To counter such degradation, the *Department of the Army* should

• Develop MCF, Ada, and the instruction-set architecture so that equipment densities will support redundant, compatible computers on the battlefield; software transportability; and adequate equipment densities to support float items, repair parts at the circuit card level, cannibalization (if necessary), test measurement and diagnostic equipment (TMDE), military computer repairmen, and the priority redistribution of critical assets (when necessary).

• Establish contracts and mobilization designee positions for technical contractor personnel whereby the civilian obtains retirement credit and Reserve pay and is called to active duty when the country mobilizes.

• Be prepared to increase reenlistment bonuses for critical computer maintenance and programer skills if the need should arise.

• Convert fixed theater computer sites to mobile sites as soon as possible.

• Review security requirements, particularly of combat service support units, to ensure the collections of computer emissions and communication transmissions are unclassified.

• Establish a computer program evaluation group to take advantage of the peacetime application of unit developed commercial computer programs (Apple, Sycor, etc.). Assign a specific unit responsibility to develop and test applications programs and, thus, eliminate the need to create duplicate programs for units with identical equipment.

# APPENDIX
# A CASE IN POINT: THE THEATER ARMY SUPPLY SYSTEM

Chapter 1 focused on the computer and factors affecting its survivability in a wartime environment. This appendix narrows the focus to computers vital to the successful operation of one important function, supply, assuming there are lessons to be learned from a mature system.

The following review of the supply system elaborates on (1) computer employments within the theater supply organization, (2) the personnel required and the training necessary for performing the supply mission, and (3) the wartime survivability of the supply system.

## THEATER SUPPLY SYSTEM OVERVIEW

Today, the US supply system has an enormous functional dependence on the computer; in fact, the computer is such an integral part of supply operations that the supply system's survivability is in doubt without it. The total force (Active and Reserve Components (National Guard and Army Reserve)) plays a major role in the theater supply system, a system that includes the receipt, issue, and storage of supplies to all units throughout the theater of operations. This supply system consists of all classes of supplies except class VIII (medical supplies), class I (perishable subsistence), and class III (bulk petroleum):

*Class I*—Subsistence, including gratuitous health and welfare items.

*Class II*—Clothing, individual equipment, tentage, tool sets and tool kits, handtools, administrative and housekeeping

supplies and equipment. Includes items of equipment, other than principal items, prescribed in authorization/allowance tables and items of supply (not including repair parts).

*Class III*—Petroleum fuels, lubricants, hydraulic and insulating oils, preservatives, liquid and compressed gases, chemical products, coolants, deicing and antifreeze compounds, together with components and additives of such products and coal.

*Class IV*—Construction materials to include installed equipment and all fortification/barrier materials.

*Class V*—Ammunition of all types (including chemical, radiological and special weapons), bombs, explosives, and mines, fuses, detonators, pyrotechnics, missiles, rockets, propellents, and other associated items.

*Class VI*—Personal demand items (nonmilitary sales items).

*Class VII*—Major end items, a final combination of end products which is ready for its intended use (principal item), e.g., launchers, tanks, mobile machine ships, vehicles.

*Class VIII*—Medical material, including medical-peculiar repair parts.

*Class IX*—Repair parts and components to include kits assemblies and subassemblies (reparable and nonreparable) required for maintenance support of all equipment.

*Class X*—Materiel to support nonmilitary programs, e.g., agriculture and economic development not included in classes I through IX.

## THE EMERGENCE OF AUTOMATION

Through the early 1950s, the Army Supply System consisted of manual requisitions, stock record cards, locator cards, and tub files. The soldier with a stubby pencil, the keystone of the theater supply system, maintained the manual supply records, which consisted of over one million line items worth millions of dollars. The proper issue, receipt, and stor-

age of theater supplies relied on the accuracy of these manual files and on the soldier who updated the records and files on a daily basis. Inaccuracies occurred through incorrect postings and arithmetic errors. Periodically, manually recorded onhand balances were validated by wall to wall inventories. More often than not, the records required adjustment.

To reduce posting and arithmetic errors, in the late 1950s, the Army began to convert some of its inventory control point manual records to electronic accounting machine (EAM) card files and listings. In 1960, these EAM card files and listings were converted to the newly introduced Moby Dick, a militarized computer that had been built by the Univac corporation.

Once introduced, computers spread rapidly throughout the Army. Second generation computers were installed at the theater and corps inventory control points, and mobile Univac 1005 computers were introduced into our divisions. The computer became a status symbol. More and more automated functional systems were fielded as functional managers moved to automate manual procedures. Unfortunately, these fielded systems were developed in isolation from one another; the systems became pieces in a puzzle, but they could not be interlocked.

As noted in chapter 1, this disjointed systems proliferation forced congressional involvement that resulted in the passage of the Brooks Bill. In response to this bill, the Army tried to use its computer resources more efficiently. Responsibilities for computer system design and development were stripped from the functional expert and transferred to computer design centers under the auspices of computer resource managers.

The early 1970s witnessed third generation computers replacing the older hardware. Unfortunately, much of the software remained unchanged. To avoid costly software reprograming, a computer software package was developed to enable the use of the old computer programs. With this software package the old programs could process on a new computer. Other industry efforts to reduce user costs resulted in cheaper, smaller computers with more computer power—"more bang for the buck." These technological advancements

led to the development of the distributive processing concept. (In the 1980s, it is anticipated that the Army supply system will field systems which use distributive processing.)

*The Wartime—Peacetime Dichotomy.* The underlying problem in using automation in the development of Army automated supply systems is the wartime-peacetime dichotomy. In peacetime, effective and efficient use of the budget emerges as the dominant management philosophy; during wartime, dollar constraints are ignored to ensure mission effectiveness.

The Army's Automation/Communications Transition Plan defines the Combat Service Support (CSS) goal as "Do in peace what we plan to do in war. The peacetime medical, personnel, and logistical structure must be such that no major change is required when transitioning to war, and the procedures to be followed by the operators must be the same in peace and war."[1] This goal may be impossible to achieve under our existing supply system. Inherent in our current efficiency-designed system are budgeting and accounting principles that use personnel resources and computer time. During war, processing these extraneous functions along with increased personnel and computer resource requirements will quickly overload the supply system, causing the disordered distribution of supplies. The port of Saigon during the Vietnam war was an example of an overloaded system in which no one knew what supplies had arrived at the port or to whom they were consigned. The primary wartime objectives of receipt, issue, and storage of supplies were in competition with the extraneous functions, and chaos resulted.

To meet the Automation/Communication Transition Plan objective of doing in peace what we do in war, we have two supply system alternatives that avoid a chaotic situation:

- Design a wartime system separate from the current peacetime system.

- Redesign a peacetime system that moves the extraneous financial and centralized efficiency management processes to units in the theater rear or back to the continental United States.

Consider the first alternative. Congressional pressures

during a peacetime environment require the Army to retain the basic budgeting and accounting principles required for financial management. Procedures to develop files from the peacetime data to operate a streamlined wartime system must be incorporated into the current peacetime system. These wartime files would be designed around the basic supply functions of receipt, issue, and storage of supplies, because no financial management system should operate overseas during war.

History has shown that congressional pressures for financial and efficiency management subside at the outbreak of a war. Since the most critical time for system overload is at the start of a conflict, it is essential that the supply system be prepared from the start to provide only the basic functions of receipt, issue, and storage. Thus, when a war erupts, a smooth transition from the peacetime supply system to the wartime supply system can be initiated. If the war stabilizes, as in Vietnam, and Congress reasserts pressure for financial efficiency, the wartime system could revert back to peacetime efficiency controls.

In the second alternative, all financial management and centralized management functions, such as demand analysis, reconciliating, asset reporting, and asset visibility, would be transferred to the theater rear, offshore, or to the continental United States. This constitutes the creation of a new peacetime system. Under such a system, the transaction surge created by war might not cause a computer system overload in which computer capabilities to handle the increased transactions are exceeded.

A danger exists in this latter alternative. Our society uses the budget as the predominant management constraint. If this new peacetime system is inefficient, pressures will mount to make it efficient. For example, from past experience when financial controls did not exist in the division, as pressures mounted for fiscal control, divisions were provided financial targets and budgets. They were pressured to live with these fiscal targets. The effect of these actions was that dollars were managed, not squandered. The same situation will develop with this new peacetime system. Pressures will require that fiscal controls move closer to where the money is spent, and

the peacetime system will have to be changed to accommodate these pressures.

## COMPUTER EMPLOYMENTS

To better understand whether fiscal controls can be applied to units, it would help to know where the automated supply systems are located in the theater of operation. Typically, boundaries divide the theater into three distinct areas—the theater Army, the corps, and the division. Table A–1 depicts a slice of today's theater supply organizations and the computers that support the organizations. A cursory review of this table shows a computer proliferation problem; the current theater supply system contains six different computers (hardware) and eight different software packages. Plans will eventually reduce the eight different computers to three. However, each software application must be tailored to ensure compatibility with its hardware operating system. Each hardware and software combination requires different resources for maintenance. Savings could be accrued with hardware and software system reductions to one or even two systems.

In addition to the computers shown in table A–1, units in the theaters are buying microcomputers, such as the IBM Series 1, the Apple, and Sycor 500. (IBM's Series 1 is sometimes classified as a mini.) Each unit now develops command uniques to solve its problems (supply, maintenance, command and control, etc.). To correct this diffusion of effort and computer proliferation the Army should act as follows:

- Standardize computers throughout the theater of operations by establishing a compatible family of computers (a supermini and a microcomputer) and develop a standard extension package so that major commands can assume some of the extension workload.

- Field the computers faster; e.g., it took approximately 8 years to field the division IBM 360 series computers. If plans for its replacement are accurate, the division system will have been in our Active divisions from 8 to 16 years. Eight years is too long to require a systems design center to maintain two systems (Univac 1005 and IBM 360–30) for our divisions.

- Use the units in the field to help develop standard Army

systems. Establish yearly meetings on command unique developments with subsequent assignment of responsibility to a specific unit for command uniques required by several commands.

Table A–2 shows the look of theater supply systems and their computers in 1986. If scheduled extensions proceed as planned, approximately 90 percent of the Active Army supply computers in the theater will be modernized with standard compatible computers. These modern computers will provide Active Army units with vertical and horizontal software transportability.

Unfortunately, only 50 percent of the Reserve component (RC) units will receive modern computers by 1986. This is a fielding plan that will create an Active/RC compatibility problem under mobilization. For example, the RC divisions have 1005 computers and the Active divisions have Decentralized Automated Service Support System (DAS3) computers. If one of the RC 1005 computers were destroyed, the computer support provided by Active Army units to the RC unit would be minimal, because the Univac 1005/Division Logistics System is not compatible with the DAS3/DS4 system (DS4 is Division Standard Supply System Support). To remedy this mobilization compatibility problem, the RC forces fielding plan should be stepped up to provide RC divisions with DAS3 computers at the same time as Active Army divisions.

Additional comments follow and are directed toward the supply organizations—division, corps, and theater Army—and the problems and the accomplishments each is making toward achieving 1986 computer employments plans.

## DIVISIONS

*Today.* Within the division, three key organizations combine to provide supply support to the front line soldier: The Division Material Management Center, the Division Data Services Center, and the operating battalions. The material center is the manager; the data center provides the computer service to the division; and the operating battalions receive, issue, and store supplies. These organizations have existed in our divisions since 1975. In the peacetime-wartime dichotomy

**Table A-1. Theater Supply Systems and Their Computers—January 1982**

| Brigade | Division and Separate Brigade | Corps | Theater |
|---|---|---|---|
| **Active Army Units** | | | |
| Manual | *Combat Service Support System (mobile)*<br>IBM 360–30 hardware with DLOGS software<br>IBM 360–30 or 40 hardware with DS4 software | *Nondivision Direct/ General Supply Support (mobile)*<br>NCR 449 and NCR 500 hardware with ledger accounting software<br>DAS3 Honeywell (A model) level 6 hardware with Phoenix software (DS4 software under test)<br>*Corp Support (mobile)*<br>IBM 370–138 hardware with SAILS ABX software<br>Corps site in Europe also | *Nondivision Direct/ General Support units (mobile)*<br>NCR 500 hardware with ledger accounting software (A model)<br>DAS3 Honeywell (A model) level 6 hardware with Phoenix software<br>*Theater level (fixed site)*<br>Pacific and Korea IBM 360 series machines with SAILS ABX software and for ammunition SAAS # 1 software<br>Europe IBM 4300 with multiple virtual storage |

**Table A-1. Theater Supply Systems and Their Computers—January 1982—Continued**

| Brigade | Division and Separate Brigade | Corps | Theater |
|---|---|---|---|
| | | also has IBM 360-series hardware | operating system and SAILS ABX software and for ammunition the software is SAAS 1 |
| | | **Reserve Component Units** | |
| Manual | *Division Logistic System (DLOGS) (mobile)*<br>Univac 1005 hardware with DLOGS software<br>Manual | *Nondivisional Direct/ General Supply Support (mobile)*<br>Manual<br>NCR 500 hardware with ledger accounting software<br>*Corps Support*<br>IBM 360–40 hardware with SAILS software | *Nondivisional Direct/ General Support Units*<br>Manual<br>NCR 500 with ledger accounting software (very few available)<br>*Theater level*<br>One IBM 360–40 system for training purposes otherwise all are manual<br>Manual |

*Source:* US, Department of the Army, Project Manager, Tactical Management Information System, "Acquisition Plan for DLDED," 2 January 1981.

**Table A-2. Theater Supply Systems and Their Computers—1986**

| Brigade | Division and Separate Brigade | Corps | Theater |
|---|---|---|---|
| **Active Army Units** | | | |
| *Forward Support (mobile) BN's*<br>DLDED hardware with edit functions input device for other functions not determined to DAS3 | *Combat Service Support (mobile)*<br>DAS3 hardware (B model) with DS4 software<br>DLDED hardware for editing input device, other functions not yet determined | *Nondivisional Direct/ General Support (mobile)*<br>DAS3 (A model) with DS4 software<br>*DLDED for editing* input device, other functions not yet determined<br>*Corps Support (mobile)*<br>DAS3 (B model) with SARSS software and ammunition software and<br>DLDED hardware for editing input device, and for ammunition (SAAS4 software); other functions not yet determined | *Nondivisional Direct/ General Support (mobile)*<br>DAS3 (A model) with DS4 software<br>DLDED hardware for editing, other functions not yet determined<br>*Theater Support (mobile)*<br>DAS3 hardware (B model) with SARSS software and software for ammunition SAAS 1<br>DLDED hardware for ammunition supply points with SAAS4 software also for editing input device and other functions not yet determined |

**Table A-2. Theater Supply Systems and Their Computers—1986—Continued**

| Brigade | Division and Separate Brigade | Corps | Theater |
|---|---|---|---|
| **Reserve Component Units** | | | |
| Manual<br>National Guard Round out brigades will receive DLDED for editing and an input device to DAS3 | *Combat Service Support (mobile)*<br>DAS3 hardware (B model) with DS4 software<br>Univac 1005 with DLOGs software until replaced by DAS3<br>DLDED serve as editing and input devices | *Nondivisional Direct/ General Support (mobile)*<br>Manual<br>DAS3 (model A) with DS4 software and for ammunition SAAS3 software DLDED serve as editing and input device to DAS3<br>*Corps Support*<br>DAS3 hardware (B model) with DS4 software<br>For ammunition DAS3 hardware with SAAS3 software<br>DLDED for edit, input device to DAS3 and | *Nondivision Direct/ General Support Units (mobile)*<br>DAS3 (A model) with DS4 software and for ammunition SAAS3 software DLDED serve as editing and input device to DAS3<br>*Theater Support*<br>Manual<br>DAS3 hardware with SARSS software DAS3 hardware for ammunition with SAAS3 software<br>DLDED for edit, input device to DAS3 and for ammunition DLDED with SAAS4 software |

**Table A–2. Theater Supply Systems and Their Computers—1986—Continued**

| Brigade | Division and Separate Brigade | Corps | Theater |
|---|---|---|---|
| | | for ammunition DLDED with SAAS4 software at the supply points | 360–40 with SAILS ABX software |

*Source:* Department of the Army, Project Manager, Tactical Management Information Systems, "Acquisition Plan for DLDED," 2 January 1981.

the centralization of the supply management function at the division material center and decentralization of operations at the operating battalions represent the Army's attempts to minimize cost and to maximize effectiveness in peacetime. This centralized organization has never functioned during war.

Prior to the existence of the division material center and data center, total responsibility for supply management and operations was decentralized to the operating battalion. Operating battalions are located under the division support command and refer to the supply and transport, maintenance, and medical battalions. In an independent brigade the operating battalion would be called a support battalion. This decentralized system has survived several wars. Under this system all resources are assigned to the person responsible (battalion commander) for providing specified mission support to the soldier.

*Tomorrow—1986.* As noted in chapter 1, the trend is to return computer operations to the functional user; the computer becomes a tool for the functional manager to use in accomplishing the assigned mission. Similarly, planned division DAS3 and division level data entry device (DLDED) extensions will provide these computer tools to the supply operator and manager. The DLDED will be located with the supply operator, the individual who receives, issues, and stores supplies. (No longer will data have to go to the division material center for key punching before the data enter the computer.) The DAS3 will be located with the supply manager. These two systems, the DLDED and DAS3 computers, will provide division computer redundancy for the first time. In addition, the DLDED test results indicate that DLDED will improve mission performance as follows:

- Process requisitions through the system approximately 84 percent faster.
- Reduce the error rate to about one-tenth of the total tested.
- Allow the supply clerk to successfully operate the system.
- Reduce lost requisitions by nearly 100 percent.

• Replace less reliable equipment (marksense forms, punch cards, interpreters, and sorters).[2]

The division material center retains supply management responsibilities and gains the computer operations responsibility; the data center loses the DAS3 computer but retains the computer systems analyst and programers. Such an organization satisfies the peacetime requirement by centralizing programer and analyst assets for the division's DAS3 and DLDED computers and takes a step toward decentralization by placing DLDEDs with the operating and support battalions as far forward as the brigade trains. (The Army now refers to DLDED as the Tactical Army Combat Service Support computer system (TACCS).) Supply managers agree that decentralization is required to maximize wartime effectiveness. The question is how much of the supply management function should be decentralized.

A step toward decentralization should include keeping the division material center in peacetime but in war moving it to the corps area and delegating many of the center's functions to the operating battalions. When we go to war the division material center's issue, receipt, and storage (management) functions and corresponding personnel would revert to the supply and transport battalion and the maintenance functions and personnel would revert to the maintenance battalion. Along with division material center and data center elements, the DAS3 computer would revert to the corps material center for operational control, but the division material center would be designated to provide property accountability and supply and maintenance management support to the division.

Essential supply and maintenance functions must be programed on a DLDED computer located in the operating battalions. This concept increases redundancy and survivability in the division as well as in the corps. Furthermore, it equips the person responsible (the supporting battalion commander) with support so that the soldier can accomplish the mission.

## CORPS

*Today.* Supply functions become much more specialized at the corps and theater levels. Here, supply units are tailored

to accomplish specific supply functions. In the corps, the supply units consist of the Material Management Center and nondivisional direct and general support units (DS/GSU). As shown in table A-1, the corps material centers are supported by IBM 370-138s and in Europe by two additional 360-40 computers. DS/GSUs are manual, supported by an NCR 500, supported by a DAS3 computer, or are being converted to the DAS3 computer. (DS/GSUs, nondivisional, provide direct or general support on an area basis to the corps or Army and backup support to the divisions in the respective corps boundaries.)

The DS/GSU supported by the NCR 499 and NCR 500 computers had difficulty in keeping these computers operational. Because of their age repair parts for the NCR 499/500 were hard to obtain; consequently, down times were lengthy. This is a danger associated with buying commercial computers that are no longer produced or maintained for the commercial market by their manufacturers.

Before obtaining the IBM 370-38 for the corps material center, the Army conducted the Automation of Wartime Functional Supply Requirements Study which concluded that the corps supply system was not wartime capable.[3] The study showed that not only were the computers incapable of handling the overload created by the transition from a peacetime to wartime posture, but also the Standard Army Intermediate Logistics System (SAILS ABX) software was inefficient and adding more work to the already overloaded system. The interim decision was made to provide the corps the 370-138 until the B model of DAS3 could be fielded and to initiate a project to redesign the SAILS ABX software.

*Tomorrow—1986.* With the fielding of DAS3, computer operations for the corps material center the Standard Army Ammunition System Level 3, and the DS/GSU will be turned over to the functional personnel for operation (table A-1). The material center SAILS software will ultimately be reprogramed as both an interactive and batch processing standard Army Retail Supply System (SARSS). Selected remote data entry devices will also provide for off-line and interactive processing. The level 3 ammunition supply processing system, which maintains ammunition onhand balances and computer author-

ized supply levels, will be developed for DAS3. It will be compatible with the theater ammunition supply system level 1, and the ammunition supply point system, level 4, located close to its supported division. The level 4 system will be programed to run on the DLDED. For level 4 to provide maximum benefit to the Army, it must have communications links to the level 3 system and the Division Ammunitions Officer. Communication, as well as ammunition shortfalls, can be transmitted to corps or division as required. Without communication, the level 4 DLDED is only a calculator.

In the planned design of SARSS, serious consideration must be given to moving the fiscal and supply management noncritical functions away from the battlefield to the corps, theater Army, or to the continental United States. Some of the functions to be moved from the division, or even the corps, during war are as follows:

- Status and reconciliations.
- Catalog related function.
- Asset visibility and accountability reporting.
- Financial management.

**THEATERS**

*Today.* The nondivisional DS/GSUs located in the theater are in the same position of modernization as the corps units (table A–2). Theater Army automation consists of the IBM 4300 and 360 series computers. Operating system software for the 4300 is being changed to multiple virtual storage. Current theater Army computer survivability is questionable. First, the computers are housed in fixed sites which are much more vulnerable to attack than mobile sites. Army plans to eventually convert the fixed sites to mobile ones. Secondly, the IBM 4300 contains the MVS operating system. If the IBM 4300 is damaged or destroyed, the corps IBM 370–138s will be unable to assume the 4300's functions, because the 370–138s are not large enough to handle the MVS operating system of the IBM 4300. The supply software package that supports the theater Army computer is SAILS ABX.

*Tomorrow—1986.* The development of SARSS and re-

placement of the IBM 4300 with DAS3 (B models) will provide horizontal and vertical compatibility with the rest of the theater. For the future, the major concern is whether SARSS can be completed on schedule. If it cannot the incompatibility that exists today will continue beyond 1986.

If new initiatives, such as demand analysis, status and reconciliations, catalog function, financial management, and asset visibility and accountability functions, are taken over at the theater Army level, the theater Army will need more computers. If these functions can be moved to the theater level, there is reason to ask why they can't be moved to the continental United States. Some functions can be moved offshore, practicularly the catalog and financial management functions. These functions are not mission sensitive; thus, historical transaction tapes can be delivered to the continental United States by courier for production runs and outputs. If needed, financial reports can be returned to the theater for review and action.

## RESERVE COMPONENTS

*Today.* Supply organization and computer employment for D+30 Army Reserve Components (RC) are planned to eventually mirror the Active Army. As long as the Army buys commercial off-the-shelf computer equipment, it is doubtful that RC units will ever have equipment compatible with Active Army units. By the time the RC units get a computer that has been in Active units, the Active units are fielding a new computer. RC units have consistently lagged from 5 to 15 years behind Active units in compatible computers. For example, GSUs in the Active Army have had NCR 500s for about 14 years; only a couple of RC units have even received the NCR 500 computer. Also, Active Army divisions have had the IBM 360–30 computer for about 14 years; no RC divisions have ever received the IBM 360–30. Even with our D+30 units, time delays to modernize these RC units are dependent upon the unit's mission. As shown in table A–2, plans are intended to provide RC supply organizations with DAS3 hardware and software.

Currently the D+10 RC divisions are equipped with Univac 1005 computers, while Active Army divisions are

equipped with IBM 360–30 computers. Under a mobilization, the D+10 units will be deployed throughout the theater, but the RC plans to deploy its divisions without the Univac 1005. Since the division material center and the supply and transport battalion are organized to process automated data, the divisions will have to reorganize and increase the strength of these units for manual operations. On the other hand, if the RC divisions did deploy with the 1005 computers and if the 1005 computers were destroyed or damaged, backup support would have to be provided by other Active or RC divisions. The lack of repair parts for the 1005 could cause this backup support to continue indefinitely. Based on the 1005 capability of servicing only one division, the backup capability from other RC divisions would be inadequate.

The D+30 corps nondivisional GS/DS units are being converted from manual and the NCR 500 to DAS3 organizations. Other RC theater units are manual except for selected corps material centers which are equipped with IBM 360–40 computers.

*Tomorrow—1986.* By 1986 most D+30 units will be equipped with mobile DAS3 computers. Other units will still be manual or will be in the conversion process to mobile DAS3 computers. Lack of funds is the major drawback to a computer compatible whole Army concept.

## PERSONNEL

The problems and progress made in fielding compatible computers to operate the supply function in the theater are only part of the case in point. To complete the picture, the following focuses on the space authorizations and the personnel required to operate the computers.

### UNIT SPACES

During the 1960s, a cost effectiveness analysis had to be performed before authority was granted to purchase ADP equipment. A personnel evaluation was an integral part of the analysis. In fact, if the personnel analysis did not show a potential personnel savings in converting from manual to an automated operation, the chances of obtaining computer purchase authority were slim. This personnel savings philoso-

phy assumed that automated supply operations would never have to revert to the manual system. The following division and corps examples show the results of personnel impacts on our supply organizations if, due to EMP or other wartime conditions, our supply units were to revert to manual operations:

*Division.* Prior to 1975, the authorization document for the headquarters and headquarters company (TOE 29-6H) of the supply and transport battalion authorized 22 additional personnel spaces for performing class II, IV, and VII supply missions if division supply operations were not automated under the Univac 1005 computer.[4] In 1975 the Army reorganized the division supply organizations by activating the division material center. It absorbed the supply management functions and the personnel (63) from the supply and transport battalion. The 63 personnel lost were absorbed in lines 1 through 8 of the division material center TOE 29-3H (on 17 November 1975). See table A-3. Since all division material centers were automated, the 22-space battalion augmentation for manual operations was dropped and a 14-man section was added to the division material center TOE. The net effect was a loss of eight augmentation spaces, which is acceptable provided the ADP equipment is completely survivable and the unit will not have to revert to manual operations. However, ADP is not totally survivable. So, the section cannot perform its mission under manual procedures with only 64 percent (assuming the division material center is at 100 percent fill) of its authorized prior automation strength. Sustained manual supply operations would surely result in a degradation in mission supply support.

*Corps/Theater.* The same problem that exists in the division also exists in corps and theater Army nondivision DS/GS units. In a comparison of the changes in the supply and service company (TOE 29-147H5) which resulted from the DAS3 automation of the manual system, automation of the DS unit causes the unit to lose 11 spaces. The spaces lost are those that would be required to sustain the nondivisional DS unit in a manual mode operation (table A-4).

As a response to the manpower and dollar constraints in the Army and the vulnerability of our computers, the Army must act as follows:

**Table A-3. Division Material Management Center—TOE 29-3H**

| Line | Section/Branch | Level | Number |
|---|---|---|---|
| *CTRHQ* | | | |
| 01 | | O5 | 1 |
| | | O4 | 1 |
| | | WO | 2 |
| | | E9 | 1 |
| | | E8 | 2 |
| | | E6 | 1 |
| | | E5 | 1 |
| | | E4 | 3 |
| | | E3 | 2 |
| | | | 14 |
| 02 | Class I and VI Section | | |
| | | O3 | 1 |
| | | E7 | 1 |
| | | E4 | 2 |
| | | | 4 |
| 03 | Class III Section | | |
| | | O3 | 1 |
| | | E7 | 1 |
| | | E4 | 2 |
| | | | 4 |
| 04 | Class V Section | | |
| | | O4 | 1 |
| | | WO | 1 |
| | | E8 | 1 |
| | | E7 | 1 |
| | | E6 | |
| | | E5 | 2 |
| | | E4 | 2 |
| | | | 8 |
| 05 | Property/Asset Accounting Branch | | |
| | | 04 | 1 |
| | | E6 | 1 |
| | | | 2 |
| *DMMC2* | | | |
| 06 | Regulations Edit Document Control Branch | WO | 1 |

**Table A-3. Division Material Management Center—TOE 29-3H—Continued**

| Line | Section/Branch | Level | Number |
|---|---|---|---|
| | | E6 | 1 |
| | | E5 | 1 |
| | | E4 | 3 |
| | | | — |
| | | | 6 |
| 07 | Management Asset Accounting Branch | | |
| | | O3 | 1 |
| | | WO | 6 |
| | | E8 | 1 |
| | | E7 | 7 |
| | | E6 | 2 |
| | | E5 | 3 |
| | | E4 | 7 |
| | | E3 | 3 |
| | | | — |
| | | | 30 |
| 08 | Reports Branch | | |
| | | WO | 1 |
| | | E7 | 1 |
| | | E4 | 2 |
| | | | — |
| | | | 4 |
| 09 | Class II, IV and VII Sections | | |
| | | O4 | 1 |
| | | E8 | 1 |
| | | E7 | 6 |
| | | E6 | 1 |
| | | E4 | 4 |
| | | E3 | 1 |
| | | | — |
| | | | 14 |
| 10 | Class IV Section | | |
| | | O4 | 1 |
| | | E8 | 1 |
| | | E4 | 1 |
| | | | — |
| | | | 3 |
| *DMMC3* | | | |
| 11 | Document Control-Edit Branch | | |
| | | E7 | 1 |
| | | E6 | 1 |

**Table A-3. Division Material Management Center—TOE 29-3H—Continued**

| Line | Section/Branch | Level | Number |
|---|---|---|---|
| | | E5 | 1 |
| | | E4 | 2 |
| | | E3 | 1 |
| | | | — |
| | | | 6 |
| 12 | Support Management Branch | | |
| | | WO | 1 |
| | | E8 | 1 |
| | | E7 | 6 |
| | | E5 | 5 |
| | | E4 | 6 |
| | | | — |
| | | | 19 |
| 13 | Maintenance Section | | |
| | | O4 | 1 |
| | | O3 | 4 |
| | | E8 | 1 |
| | | E7 | 3 |
| | | E6 | 3 |
| | | E4 | 1 |
| | | | — |
| | | | 13 |
| 14 | Company HQ Section | | |
| | | O3 | 1 |
| | | E8 | 1 |
| | | E7 | |
| | | E6 | 1 |
| | | E5 | 2 |
| | | E4 | 4 |
| | | E3 | |
| | | | — |
| | | | 9 |
| *DMMC4 Augmentations* | | | |
| 12 | Maintain | | |
| | | E4 | 4 |
| | | | — |
| | | | 4 |
| 14 | Company HQ Section | | |
| | | E7 | 1 |
| | | E6 | 2 |

**Table A-3. Division Material Management Center—TOE 29-3H—Continued**

| Line | Section/Branch | Level | Number |
|---|---|---|---|
| | | E4 | 3 |
| | | E3 | 1 |
| | | | — |
| | | | 7 |
| | Total | | 147 |

• Increase unit strengths with wartime augmentations until our computers are no longer vulnerable or establish cellular teams in the theater to assist units in a manual mode (put some teams into the active structure and the rest into wartime augmentations).

• Commit research and development dollars to improving computer tolerance to EMP and making shelters invulnerable to EMP.

• Continue to build redundancy into the theater units and systems by standardizing computers and functional systems.

Also worthy of discussion is the need for a courier. Currently, units are required to use authorized supply personnel to perform courier functions. When a supply person is used as a courier, his or her primary job suffers. And, the time couriers will spend away from their primary jobs will increase as the Army moves as follows:

• Toward a distributive processing system without radio or wire communications capabilities. Records must be transfered often from operating battalions to the material center and between the division material center and the corps material center.

• Its financial management and other centralized supply management functions further to the theater rear, increasing courier requirements.

To resolve this courier shortfall in supply organizations, augmentations should be built into the supply TOEs until the communication system can accommodate supply teleprocessing requirements.

## REENLISTMENTS

More computers will require more computer operators, programers, and repairmen. In logistics alone the army is planning on fielding more than 1,000 additional computers by 1986; DOD has reason to be concerned about the availability of programers. See figure A–1. The demand for Army programers is expected to increase to 125,000, while the number of computers in use will top the 250,000 mark by 1985.[5] To assess the Army's ability to meet these computer operator, programer, and repairman skills demands, a review of calendar 1981 reenlistment (REUP) rates of these MOSs is useful. In table A–5 three computer military occupational specialties are compared to the average initial, midterm, and career REUP rates of all Army military occupational specialties.

Since the 34C MOS is new and requires an E4 entry level, which means the soldier will have been in the Army in another MOS for a tour, no figures are available for first termer REUP rates. In table A–5 a comparison of specific computer MOS REUP rates and the Army *average of all computer* MOSs shows the midterm computer repairmen as a serious problem and 74F computer programer at midterm and careerist REUP as a potentially serious problem. Authority to establish REUP bonuses for 74F and 34C MOSs could provide a stabilizing effect to ensure adequate reenlistments for future unit assignments and reduce the Army's overall programing costs. Figure A–2 shows that software costs appear to be doubling every 5 years.[6] With this condition in mind, the Army needs to retain experienced, more productive programers. A REUP bonus could save a half-year of training time and retain a productive programer.

## CIVILIAN ADP PERSONNEL

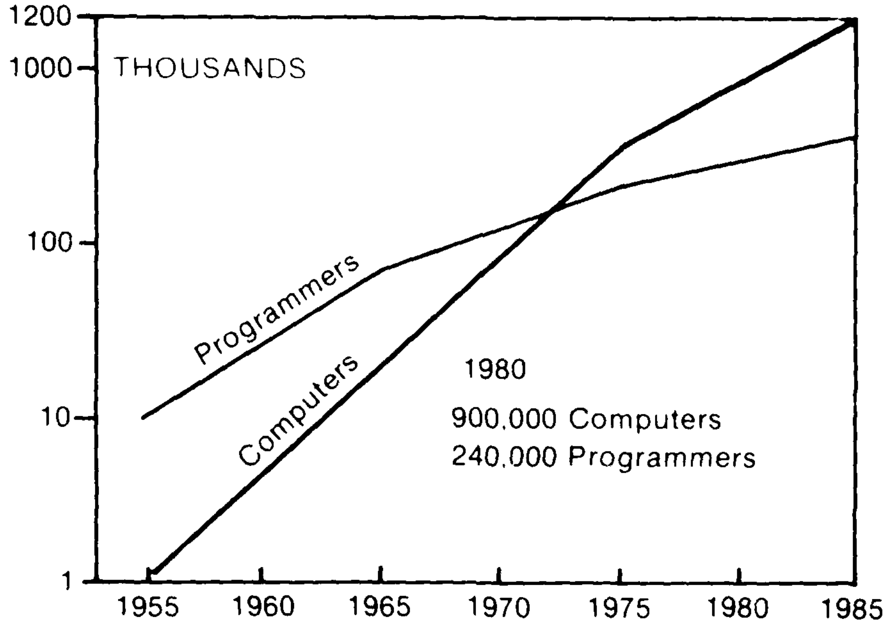
In some theaters, certain unit missions, such as materiel management and engineering maintenance, are performed by civilians under host nation support agreements and by US civilian civil service Government workers and contractors. Under host nation and US civilian civil service agreements with the United States, the host nation or the US civil servant pledges in writing to continue to work for the United States even if a conflict breaks out. Although not foolproof, the Army

## Table A-4. Sample of Unit Space Changes Following DAS3 Automation

### Supply & Service Company (DS)

| Current | | | | Proposed DAS3 Organization | | | |
|---|---|---|---|---|---|---|---|
| Description | Grade | MOS-ASI | Spaces | Description | Grade | MOS-ASI | Spaces |
| *Sup & Svc Ops Office* | | | | *Sup & Svc Ops Office* | | | |
| Operations Officer | LT | 02A00 | 1 | Operations Officer | LT | 92A00 | 1 |
| Laundry NCO | E7 | 57E40 | 1 | Laundry NCO | E7 | 57E40 | 1 |
| Materiel Supply Supv | E7 | 76D40 | 1 | Clerk Typist | F3 | 71L10 | 1 |
| Supply Control Supv | E7 | 76P40 | 1 | Supply Support Tech | WO | 762A0 | 1 |
| Supply Con/Acct Clerk | E5 | 76P20 | 3 | DAS3 Computer Repairman | E6 | 34C30 | 1 |
| Card Punch Operator | E4 | 74B10 | 1 | Mat Con & Acct Sp | E5 | 76P20–U8 | 1 |
| Clerk Typist | E3 | 71L10 | 1 | DAS3 Computer Repairman | E5 | 34C20 | 1 |
| Supply Con/Acct Clerk | E4 | 76P10 | 9 | Mat Con & Acct Sp | E4 | 76P10–U8 | 4 |
| Card Punch Operator | E3 | 74B10 | 1 | Mat Con & Acct Sp | E3 | 76P10–U8 | 2 |
| Clerk | E3 | 71L10 | 1 | Mat Con & Acct Sp | E6 | 76P30–U8 | 1 |
| Supply Con/Acct Clerk | E3 | 76P10 | 5 | | | | |
| | | | 25 | | | | 14 |

*Source:* US, Department of the Army, TOE 29–147 H5, dated 31 July 1975, with seven changes.




*Source:* US, Department of Defense, "DOD Digital Data Processing Study," October 1980.

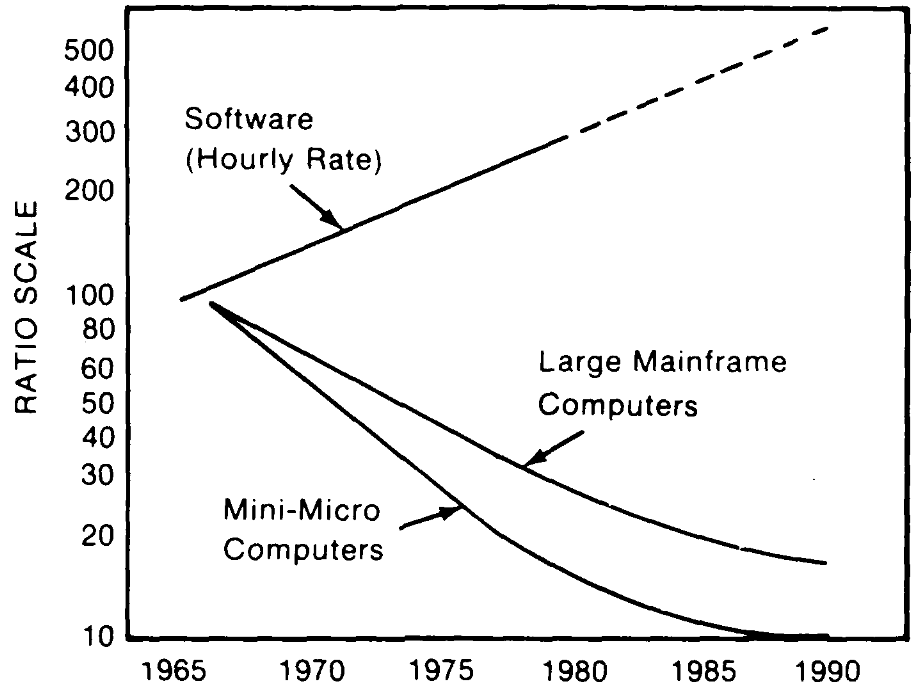
**Figure A-1. DOD Computers and Programers**

has used civil service civilians with satisfactory results in oversea theaters during war. Contract workers, on the other hand, are not bound by their companies. The example of the IBM repairmen in chapter 1 amply makes the point that in critical areas, such as computers, petroleum, and ammunition, the Army must strengthen its organic capabilities to assume its wartime missions.

**Table A-5. 1981 Calendar Year Reenlistment Rates**

| MOS | Function | Initial (1st REUP) | Midterm (10 yr) | Careerist (over 10 yrs) |
|---|---|---|---|---|
| 34C | Repairmen | 0 | 40% | 100% |
| 74D | Operator | 51% | 67% | 87% |
| 74F | Programer | 57% | 59% | 77% |
| 1981 | Average of all MOS(s) | 55% | 75% | 96% |

*Source:* US, Department of the Army, Deputy Chief of Staff for Personnel, "487 Report," as of fiscal year ending 1981.




*Source:* US, Department of Defense, "DOD Digital Data Processing Study," October 1980.

**Figure A–2. Software Is Labor Intensive**

Even if we strengthen our TOE units by identifying and converting critical positions to military, there still exists a post-deployment support problem. Using computers as an example, a surge in requirements created by wartime demands on existing computer hardware and software systems will cause a fluctuating demand for post-deployment software assistance teams to assist in trouble shooting system failures. Because of the required computer expertise, these post-deployment software assistance teams will have to be made up of contractors or civil servants. To ensure the availability of these personnel or similar critical skills personnel, these critical positions should be identified as mobilization designee positions. Qualified civilian personnel should be recruited and signed as mobilization designees so that if a war developed, mobilization designees would be available to keep the automated systems functioning.

## RESERVE COMPONENTS

During a war, if automated RC units were forced to revert to manual operations, the RC units would experience the same personnel shortages as the Active forces, since RC automated units contain the same authorization structure as Active Army units. As of February 1982, sufficient personnel are enlisting for computer operators and programers. (See table A–6.) In fact, RC computer operators and programers are overstrength 10 and 27 percent, respectively. (It's too early to tell about the 34C MOS (repairmen).) To date only one RC unit has been reorganized under the DAS3 structure.

**Table A–6. Reserve Component Computer Personnel Authorizations and Assets as of February 1982**

| MOS | Computer Function | Authorized | Assigned |
|---|---|---|---|
| 74D | Operator | 730 | 800 |
| 74F | Programer | 197 | 252 |
| 34C | Repairmen | 2 | 3 |

## TRAINING

Training personnel to use the rapidly increasing number of computers in the supply system is a major task. For automated supply systems, the training must include functional as well as computer training. Generally, effective training is provided via functional and specialized automated courses. Problems do occur, not so much from the lack of automated systems training as from the improper use of the trained personnel. In reviewing the training problem, the following examines officer, enlisted, and RC courses and assignment procedures.

## OFFICERS

Computer management philosophies for the mid-1980s are changing. With the advent of cheaper, smaller computers, functional personnel are once again managing their own computer operations in a current management trend toward decentralization. For example, the division supply organizations

will be provided a minicomputer (DAS3s) at the division material command and microcomputers (DLDEDs) throughout the division support command's operating battalions.

Under this movement to decentralize, supply officers will have computers under their direct control. For officers entering the service in the supply field, Army-designed supply officer courses typically include a 19-week officer course followed by a career officer's course of 26 weeks. Officers entering the supply field later in their careers are provided a supply management officer's course of 9 weeks (see table A–7).

**Table A–7. Officer Training Courses**

| Courses | Career Supply Officers | Transfer Supply Officers | Warrant Officers |
|---|---|---|---|
| Basic (entry on active duty) | X | | |
| Officer Advance—26 weeks (4–8 years of commissioned service) | X | | |
| Supply Officer Courses—9 weeks | | X | |
| Warrant Advance—19 weeks (10 weeks specialized training depending on individual MOS) | | | X |
| Specialized courses for selected persons (examples: DAS3, DS4, SAILS) | X | X | X |

Unless the officers graduating from the basic and advanced courses receive a specialized systems course like DAS3 or DS4, they do not receive enough training on computer operations to be operations officers in a DAS3 organization or division material center. When the basic or advanced course graduate receives a specialized training course like DAS3, we don't know whether the graduate will be assigned as a DAS3 operations officer. For example, the TOE for a direct support supply and service company (table A–3) authorizes a lieutenant to be in charge of the DAS3 operation. The TOE position calls for a 92A00 (a supply officer), not a supply officer trained in DAS3 operations. The DAS3 trained officer receives computer operations training that the supply officer does not get.

If the Army is to ensure the proper use of its trained officers and enlisted personnel, two actions must occur:

• The Army must change authorization documents to reflect the primary and specialized skill requirements of the TOE position for officers and enlisted personnel. The authorization document allows seven spaces for skill identification. For example 92A 53 U8 is translated—the officer has a primary skill of Supply Officer (92A), an alternate skill as an ADP officer (53), and an additional skill indicator as DAS3 trained (U8).

• The Army must require the field to requisition officer and enlisted personnel using the entire nine- or six-digit requisition field. For example, for an officer the nine-digit requisition field could be 92A 53 U8 U6. The requisition field can then be matched with the authorization document to ensure the right man is being assigned to the right job. The requisition gives the added capability of identifying another additional skill indicator (U6–DS4 trained).

A review of officer training courses identified two courses with major shortcomings—the supply officer's course and the specialized DAS3 course (the only specialized course reviewed). The supply officer's course is designed for all grades. It focuses on how to do the work (fill out forms, reports, etc.) as opposed to how management uses the reports the system provides. Also, an additional field grade supply officer's course needs to be added to the course offerings. This new course for field grade officers must emphasize the use of the supply management reports for uncovering potential problems and for taking actions to correct the problems with specific policy alternatives, actions, or decisions.

The DAS3 course needs to incorporate the following additional subject material:

• Security systems.

• Continuity of operations requirements under AR 18–7.

• Procedures for interfacing with the Computer Systems Command.

**ENLISTED**

Enlisted personnel receive 100 hours, and the officers receive 66 hours training on manual systems. It is essential that

this training on manual systems continue in the officer and enlisted courses even after all the Army supply units have been automated. The manual training is particularly important for personnel holding the 76P and 76C MOSs, the soldiers who would actually be required to post manual records in war if the computers were destroyed.

In the past, conversion from automated systems to manual systems did not pose a potential problem, since the noncommissioned officers (NCO) teethed on, and grew up with, the manual supply system. With most manual supply systems now converted to automated systems, this NCO experience will diminish drastically; the training rotation base from units with manual systems to units with automated systems has disappeared. Supply units that are like the division material center and the operating battalion must continue to provide manual refresher training. Past experience in the division material center indicates that the soldiers' proficiency and ability to establish manual records are minimal. This expertise now rests with a few of our senior NCOs and officers.

**RESERVE COMPONENTS**

With the increased thrust toward automation, RC unit training problems surpass those of the Active Army. RC unit training for a year consists of 16 hours per month and 2 weeks in the summer. During these training periods, functional training takes a back seat to mandatory training requirements. Required training that is unrelated to automated systems operations engulfs nearly half of the unit's training time. Three alternatives for making RC training more effective follow—use of full-time technicians, the Sister Unit concept, and individual MOS training.

*Full-time Technicians.* Developing creative training that does not tax the existing system is difficult. The National Guard has created full-time positions in selected nondivisional DS/GS units to handle all supply transactions for state property and fiscal officers—an excellent vehicle to train nondivisional personnel. Unfortunately, of the 75 units scheduled for DAS3 by 1984, only 32 are located in different states. Other training schemes must be developed for states with more than one nondivisional DSU, such as Florida, which has four. In

such cases, the Army could develop a Sister Unit concept. The concept requires an Active Army unit to become deeply involved in totally supporting the sister RC unit in training and is similar to the round-out brigades, such as the 3d brigade of the 25th Infantry Division. Units in the division are directly responsible for assisting in all aspects of the RC unit's training. For support units, summer activations could require RC units to assume the missions of their Active Sister Unit. Actual deployments, such as Reforger missions overseas, could eventually be implemented as part of the Sister Unit concept.

*MOS Training.* Of the computer operators and programers (see table A-5) authorized in RC units, approximately 80 percent are fully qualified, trained, and proficient in their MOS. The other 20 percent either receive training on the job or in school. It is notable that the RC units are provided more quotas for attending Active Army MOS producing schools than the RC can use. In fact, quotas are turned back every year. The real glitch is that the RC soldier is a civilian first and a soldier second. The training quotas are turned back by RC units because the soldier is simply unable to be away from his or her primary civilian job for extended periods of time.

During this technological era, the Army must either develop innovative training alternatives for RC personnel or be prepared to accept a marginally trained RC force on mobilization day. The Army cannot afford to accept the latter because making an RC soldier technically proficient would take too long. We must develop a training methodology that equals our equipment technology. Alternatives to RC training that the Army can adopt follow:

• *Contract for technical MOS training with civilian agencies (universities, contractors, or computer corporations).* The Army should pay for the training, but the training should be on the soldier's time. Only in very special situations should schooling substitute for drill attendance.

• *Develop a college/contractor/Army program of instruction in which the more general technical training is provided by civilian organizations.* The Army school responsible for the

MOS would provide a traveling team to teach equipment-specific training to the RC soldiers on drill nights.

• *Set up a program to capture high school graduates.* In the program the Army would pay for tuition and books (not salary) for sending them to a technical school or a community college for an associate degree. The soldier would have to serve 3 years in the Reserves for every year of schooling.

## SUPPLY SYSTEM SURVIVABILITY

New initiatives in supply system automation will result in increasing reliance on the computer. This reliance leaves many of us in a quandary over whether or not these computerized systems can survive a war. Army attention must be directed toward the elements that increase the supply system's chance of survival. Four elements converge to increase system survivability: (1) redundancy through standardization, (2) avoidance of enemy detection, (3) system availability, and (4) responsive maintenance.

### REDUNDANCY THROUGH STANDARDIZATION

*Software Standardization.* In automated supply systems the computer represents half of the standardization problem; software is the other half. Army plans eventually call for standardization of computer software and of the functional procedures using the data output. Currently, hardware and software packages are not standardized. Neither D+10 nor Active Army divisions, singularly or collectively, have the same hardware or software. When the B model of DAS3 equipment replaces the IBM 360–30, the division and nondivision software packages (DS4 versus Phoenix) will still not be compatible. It will take 6 years to complete the DAS3 hardware fielding plan to all theater supply units in the Active Army, 8 years for the D+10 RC units, and 15 years for all RC units.

Using history as a guide, the Army will begin replacing fielded DAS3 computers in about 10 years. If commercial equipment from a different manufacturer is fielded, new software programs to link the existing software to new equipment will have to be developed. Unless equipment is totally compatible, normally not the case with equipment manufactur-

ers, a one to one transfer in software will be an insurmountable task to achieve. Thus, the new ADP procurement must plan for the transportability of software. Replacing existing automated supply systems with transportable software and hardware redundancy will provide the user with a more survivable system.

*Output Standardization.* The prudent war planner considers all contingencies, including nuclear war and the eventual destruction of a supply computer. With such possibilities in mind, it is imperative that the efficiency of our wartime module of supply systems software be tested in peacetime under simulated war conditions and modified, if necessary, to respond favorably under conditions of stress.

Peacetime fiscal constraints, requirements, and pressures dictate that the wartime module be developed from the peacetime module, not vice versa. The wartime module must contain the capability to produce output which resembles the manual records. This way, the computer output can be used as the manual record in the event the computer is destroyed; e.g., a single line item per page on the stock status report would be formatted as a manual record. Produced periodically, this reformatted report can also be used for continuity of operations training; functional managers are ensured that their units can operate in a manual mode.

## AVAILABILITY

*Mobility.* The majority of the army's theater computers are mobile, a factor which enhances survivability. This ability to relocate data processing equipment lessens the chance of enemy sabotage, targeting, and collateral damage.[7] However, the theater Army computers located at fixed sites are an exception. The current timetable (mid-1980s) for changing these theater fixed sites to mobile ones must be accelerated.

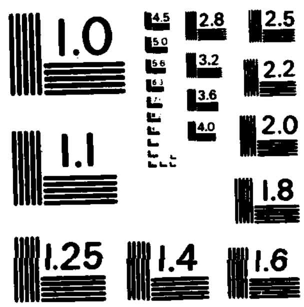
*Dispersion.* Mobility gives a connotation of dispersion. With the extension of DAS3 and DLDED hardware, the dispersion connotation of computer power on the battlefield will become a reality. Certainly, a fully developed supply systems on-line communication capability maximizes the impact of dispersion on survivability. But, currently this communication ca-

AD-A132 888 COMPUTERS ON THE BATTLEFIELD: CAN THEY SURVIVE?(U) NATIONAL DEFENSE UNIV WASHINGTON DC RESEARCH DIRECTORATE R J DEBASTIANI 1983

UNCLASSIFIED NATL SEC AFFAIRS MONO SER-83-5 F/G 9/2 NL

2/2

END
DATE FILMED
10 83
DTIC




MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS - 1963 - A

pability does not exist. New advances in communication technology for the mid-1980s can make the receipt, issuing, and processing of priority supply requirements from a data terminal to a warehouse a reality. To do so, the supply community must make immediately known the requirements for communication in the mid-1980s.

Once the communication links to upgraded DLDEDs are established, portions of the DAS3 centralized data base can be distributed, and functions can be decentralized to the operating battalions. Each operating battalion can function autonomously in this distributive processing environment to accomplish the receipt, issue, and storage of supplies for army elements. This redundancy provided by distributive systems, interconnected by communication and teleprocessing systems, makes our systems more survivable in a conventional war.

In a nuclear war, however, a distributive supply system would be insufficient alone. In addition, the Army will have to deal with EMP by hardening the computer or the shelter and by developing alternative systems, including manual operations and couriers as the communication link between distributed sites. In fact, from 1981 to 1985 user communication support requirements are expected to exceed the capabilities of a doctrinally deployed corps area communication system.[8] Reliance on couriers will be mandatory. Once communication is installed we can convert and reorient our batch processing supply system to an interactive processing one, a system that provides an immediate query capability for updating and determining current on-hand balances, due-ins, and due-outs to supply managers and operators.

## MAINTAINABILITY

The impact of hardware on supply system survivability is similar to factors covered in chapter 1. Essentially, the key factors are EMP for a nuclear conflict and repair parts, repairmen, standardization, and backup computers in both conventional and nuclear conflicts. The software impact on survivability focuses on standardization, transportability, the development and use of a wartime software module, and the formation of personnel teams in the theater and in the conti-

nental United States that are specifically organized to assist the theaters in resolving wartime supply system perturbations.

## SECURITY

Commercial computer systems implement security in an informal ad hoc manner and have been shown to be easily penetrable. Army regulations note this. In AR 380–380, *Automated Systems Security,* Army policy recognizes the inherent shortcomings of computer systems and restricts their operation to modes where security is achievable. This regulation also provides specific guidance in physical, communication, emanation, and computer security. The key to supply system security success is the enforcement of this regulation.

No requirement exists to Tempest test the DAS3 Model A hardware, since it does not process classified information. However, a situation in which the enemy knows of the stockage position of critical assets, such as ammunition, oil, barrier materials, and selective end items, might be extremely sensitive or classified. Another concern is the data from several unclassified systems that become classified if captured, assembled, and combined into a single entity (report or data base). (This is a particular concern in a division where the DAS3 B model will be employed. Therefore, it must be Tempest tested.)

*Physical.* The requirements surrounding communication, physical, and computer security for theater operation are essentially the same as for continental US operations. Command discipline, established procedures, and training will minimize security problems. Improvements that will assist any computer facility, provided the resources are made available to implement the improvements, are similar to those examined in regard to our communications in Europe (chapter 1). It is expected that command emphasis, followed by formal inspections, will provide the impetus to improve the unit's physical and computer security. Individual soldier awareness also is an important element in the unit's security program, since this will help to preclude accidental security mishaps.

*Emanation.* In accordance with AR 380–380, computers which handle secure information must pass a Tempest test to

be certified against emanation. (Tempest tests are performed on electronic equipment to ensure electromagnetic emissions are negligible; Tempest-certified equipment normally costs about twice as much as non-Tempest tested equipment.)

PRECEDING PAGE BLANK-NOT FILMED

# ENDNOTES

## INTRODUCTION

1. Alexander Ross, "Tactical Automation: The Achilles Heel of the US Army," *Armed Forces Journal* 118 (February 1981): p. 44.

## CHAPTER 1

1. US, Department of the Army Nuclear Agency, note no. 1 on EMP, June 1974.

2. US, Department of the Army Nuclear and Chemical Agency, note no. 2 on the Army Nuclear Survivability Program, January 1980.

3. Thomas A. Rose, *HEMP Study of Planned DAS3 Configuration* (Adelphi, Maryland: Harry Diamond Laboratories, June 1979).

4. Sylvania Systems, *Software EMP Protection* (Stanford, Connecticut: GTE, 30 July 1979), pp. 1–27. Also see *HEMP Study of Planned DAS3 Configuration* by Thomas A. Rose.

5. Jim Tice, *Army Times*, 23 November 1981, p. 4.

6. Industrial College of the Armed Forces, *ICAF Defense Industrial Analysis* (Washington, DC: National Defense University, May 1981), chap. 9, pp. 51–73.

7. US, Department of Defense, Defense Communications Agency, *National Communication System Technical Information Bulletin* 80–4 (June 1980).

8. Interview with Major O'Keefe, Operations Officer, Inventory Control Center, Vietnam Data Services Center, 6 January 1982.

9. US, Department of the Army, National Development and Readiness Command, DARCOM MCF "Business Plan," 19 November 1981, p. III.

10. US, General Accounting Office, GAO Report on Department of Defense Standards Program for Military Computers, "A More Unified Effort Is Needed," 18 June 1980, pp. 1–21.

11. US, Department of Defense, Deputy Secretary of Defense, memo, "Subject: Acquisition of Automatic Data Processing (ADP) Equipment and Services," 1 February 1982.

12. US, Department of the Army, Material Development and Readiness Command, DARCOM MCF "Business Plan" Strategy, 19 November 1981, Incl. 4, p. 95.

13. Colin Norman, "Microelectronics at Work: Productivity and Jobs in the World Economy" *Worldwatch Paper*, no. 39 (1980).

## CHAPTER 2

1."Improving C³ Systems and Requirements," *Signal* 35 (May/June 1981): 67–76.

2. Ross Alexander, "Tactical Automation: The Achilles Heel of the US Army," *Armed Forces Journal* 118 (February 1981): 44.

3. Ibid.

4. "Improving C³ Systems," *Signal* 35 (May/June): 67–76.

5. US, Department of the Army, Materiel Development and Readiness Command, Communications-Electronics Command, "Project Managers: Maneuver Control System (OPTADS)," *Command Review* (18 March 1982).

6. Alan B. Salisbury, "MCS: The Maneuver Control System," *Signal* 36 (March 1982): 35; A bottoms up approach to command and control development. Also see US, Department of the Army, "Project Managers: Maneuver Control System."

7. Barry Beohm, "Software Engineering," *IEEE*, C–25, (December 1976).

8. Chris Gane and Trish Sarson, *Structures Systems Analysis: Tools & Techniques* (Englewood Cliffs, N.J.: Prentice Hall, 1979), p. 213.

9. Message, HQ DARCOM to DRCDRM, 191330Z January 1982, Subject: Automation Commodity Command Study.

10. US, Department of the Army, Materiel Development and Readiness Command, Communications-Electronics Command, study, "Post-Deployment Software Support Concept Plan for Battlefield Automated Systems," May 1980.

## APPENDIX

1. US, Department of the Army, "CSS Automation/Communications Transition Plan FY 81–FY 88," 1 September 1981.

2. US, Department of the Army, Project Manager, Tactical Management Information Systems, "Acquisition Plan for DLDED," 2 January 1981.

3. US, Department of the Army, Training and Doctrine Command, Army Logistics Center, "Automation of Wartime Functional Supply Requirements," January 1980.

4. US, Department of the Army, *Headquarters and Headquarters Company of a Supply and Transport Battalion in the Armored, Infantry and Mechanized Divisions*, TOE 29-6H (Washington, DC: GPO, 30 November 1970).

5. US, Department of Defense, "DOD Digital Data Processing Study," October 1980.

6. Ibid.

7. National Research Council, *Report on Modernization, US Air Force Base Automation System, Phase IV, 1981* (Washington, DC: National Academy of Sciences).

8. US, Department of the Army, Training and Doctrine Command, Army Logistics Center, "Communications Analysis in Support of CSS Automation/Communication Transition Plan," 15 March 1982.

PRECEDING PAGE BLANK-NOT FILMED

# GLOSSARY

## SELECTED ACRONYMS

| | |
|---|---|
| CSC | Computer Systems Command |
| DARCOM | Department of the Army Material Development and Readiness Command |
| DAS3 | Decentralized Automated Service Support System |
| DDC | Division Data Center |
| DLDED | Division Level Data Entry Device |
| DLOGS | Division Logistics System |
| DMMC | Division Material Management Center |
| DSCS | Defense Satellite Communication System |
| DS/GSU | Direct Support/General Support Unit |
| DSVT | Digital Secure Voice Terminal |
| EMP | Electromagnetic pulse |
| JTIDS | Joint Tactical Information Distribution System |
| KIPS | thousand instructions per second |
| MIPS | million instructions per second |
| MOPP | Mission Oriented Protective Posture |
| MOS | Military Occupational Specialty |
| MSE | Mobile Subscriber Equipment |
| MTBF | Mean Time Before Failure |
| MTTR | Mean Time to Repair |
| PLRS | Position Location Reporting System |
| RC | Reserve Components |
| SAAS | Standard Army Ammunition System |
| SAILS | Standard Army Intermediate Logistics System |
| SARSS | Standard Army Retail System |
| SINCGARS | Single Channel Ground and Airborne Radio System |
| TACCS | Tactical Army Combat Service Support Computer System |
| TMDE | Test Measurement Diagnostic Equipment |
| TOE | Table of Organization and Equipment |
| TRADOC | Department of the Army Training and Doctrine Command |

## TERMS

*Bottom-up approach.* A systems development method which defines and builds subsystems as complete units. This method begins with the lowest level routines and then tests that the subsystems work together in an integrated system.

*Bytes.* A binary character string operated upon a unit and usually shorter than a computer word.

*Cannibalization.* The use of parts from one inoperable piece of equipment to repair another deadlined piece of equipment.

*Chip.* An integrated circuit on a silicon wafer slice.

*Command and control systems.* The facilities, equipment, communications, procedures, and personnel essential to the commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. Simply, the resources needed to control forces on the battlefield.

*Commodity command.* A DARCOM command responsible for total management of a specific DARCOM commodity.

*Computer Systems Command.* A command responsible for the development, fielding and maintenance of multifunctional, multicommand general purpose ADP systems.

*Deadlined.* Inoperable equipment.

*Decentralized Automated Service Support System.* The computer system that will standardize logistics system computer hardware in the theater of operations.

*Division level data entry device.* The Army now refers to the DLDED as the Tactical Army Combat Service Support Computer System (TACCS).

*Electromagnetic pulse.* An energy source, similar to a lightning bolt but many times greater, created by the interaction of nuclear radiation (from a nuclear burst) with ions in the atmosphere or the atmosphere and the earth's surface.

*End item density.* The number of complete pieces of equipment in a command.

*Executive function.* Controls the execution of other operating system routines and regulates the flow of work in a data processing system.

*Fault tolerant.* The ability of a system to operate effectively in spite of a component failure.

*Fiber optics.* A technique of transmitting light through long transparent fiber material, such as glass.

*Field.* To place equipment in an operational unit.

*Firmware.* Hard wired programs which interpret machine language instructions and direct the corresponding machine operations.

*Hardware*. Computer equipment used in data processing; it is able to accept and store data, execute a sequence of operations on data as opposed to computer programs, procedures, rules and associated documentation. Examples of hardware are the central processing unit, terminal, printer, tape drives, and disc.

*Instruction-set architecture*. The attributes of a digital computer or processor as might be seen by a machine (assembly) language programmer, i.e., the conceptual structure and functional behavior as distinct from the organization of the data flow and controls, logic design, and physical implementation. This definition includes the processor, input/output instruction sets, operations codes, speed of accessible clocks, interrupt structure, format and use of registers, and memory locations that may be directly manipulated or tested by a machine language program.

*Joint Tactical Information Distribution System*. The system that provides tri-service secret level secure mode communications for the battlefield.

*Maintenance float*. A reserve item issued in place of a deadlined item that has been turned in to the maintenance unit when the deadlined item is not immediately repairable.

*Military occupational specialty*. The area of specialization in which the soldier who has gained knowledge through training or on the job experience is expected to perform his duties.

*Mission oriented protective posture*. To perform an operating mission in a prescribed chemical battle dress.

*Multiple virtual storage*. The space on several storage devices that may be regarded as main storage by the user of the computing system. The size of the virtual storage is limited only by the addressing scheme of the computing system and the amount of auxiliary storage available.

*Persistent chemicals*. Chemicals which retain toxicity from several hours to several days under normal terrain and weather conditions.

*Position Location Reporting System*. The system used to provide automatic position reporting (location) of friendly units.

*Protocol*. A set of conventions between communicating processors on the format and contents of messages to be exchanged.

*SIGMA*. The force level integrated command and control system.

*Software*. Computer programs, procedures, rules, and associated documentation concerned with the operation of a data processing system.

*Standard Army Intermediate Logistics System*. The logistics system between the division and the DARCOM wholesale system.

*Standard Army Retail System*. The system which will replace SAILS.

*Table of organization and equipment.* The authorization document for military uniformed units with a military combat, combat support, or combat service support mission.

*Tactical Army Combat Service Support Computer System.* Also called the division level data entry device (DLDED).

*Theater of operations.* That portion of an area of conflict outside the continental United States that is necessary for offensive or defensive military operations.

*Top down approach.* A systems development method that defines the major objectives/functions and decisions to be achieved and then proceeds in the identification of the lesser function; models the information flow planning for the integration of subsystems.

## NATIONAL SECURITY AFFAIRS MONOGRAPH SERIES

*(See page ii for ordering information.)*

83–4 *The Chinese People's Militia and the Doctrine of People's War.* Thomas C. Roberts. (GPO)

83–3 *Improving US Theater Nuclear Doctrine: A Critical Analysis.* Jerry M. Sollinger. (GPO)

83–2 *US Strategy to Counter Domestic Political Terrorism.* James B. Motley. (GPO)

83–1 *The Sixteenth Nation: Spain's Role in NATO.* William L. Heiberg. (GPO)

82–7 *Coping with Change: United States Policy Toward South Africa.* Scott Fisher (GPO)

82–6 *Logistics Over the Shore: Do We Need It?* Dan J. Beakey. (GPO)

82–5 *Base Development and the Rapid Deployment Force: A Window to the Future.* Lewis C. Sowell, Jr. (AD No. A122833) (GPO)

82–4 *US Space System Survivability: Strategic Alternatives for the 1990s.* Robert B. Giffen. (AD No. B069357) (GPO)

82–3 *Soviet Intentions and American Options in the Middle East.* Benson Lee Grayson. (AD No. A118663) (GPO)

82–2 *The German Army and NATO Strategy.* Stanley M. Kanarowski. (AD No. A122372) (GPO)

82–1 *Nuclear Proliferation in the Middle East: Implications for the Superpowers.* Roger F. Pajak. (AD No. A121852) (GPO)

81–3 *Accelerated Production: The Air-to-Air Missile Case.* John C. McLaurin. (AD No. A119759) (GPO)

81–2 *Nuclear Testing and National Security.* Roger N. Fritzel. (AD No. A121032) (GPO)

81–1 *Ballistic Missile Defense and Deceptive Basing: A New Calculus for the Defense of ICBMs.* Raymond E. Starsman. (AD No. A104391) (GPO)

80–9 *Construction Support for Mobilization: A National Emergency Planning Issue.* Edward G. Rapp. (AD No. A094251) (GPO)

80–8 *Defense Management in the 1980s: The Role of the Service Secretaries.* Richard J. Daleski. (AD No. A095558) (GPO)

80–7 *Peacetime Industrial Preparedness for Wartime Ammunition Production.* Harry F. Ennis. (AD No. A089978) (GPO)

80–6 *Oceania and the United States: An Analysis of US Interests and Policy in the South Pacific.* John C. Dorrance. (AD No. A089120) (GPO)

80–5 *Roland: A Case For or Against NATO Standardization?* Daniel K. Malone. (AD No. A084881)

80–4 *Commitment in American Foreign Policy: A Theoretical Examination for the Post-Vietnam Era.* Terry L. Deibel. (AD No. A084965) (GPO)

80–3 *A United Front Against Hegemonism: Chinese Foreign Policy into the 1980's.* William R. Heaton, Jr. (AD No. A082321) (GPO)

80–2 *The Philippine Bases: Continuing Utility in a Changing Strategic Context.* Lawrence E. Grinter. (AD No. A082320)

80–1 *The Future of Jerusalem: A Review of Proposals for the Future of the City.* Lord Caradon (Sir Hugh Foot). (AD No. A082319) (GPO)

## THE RESEARCH DIRECTORATE

The Research Directorate provides a sustained opportunity for uniformed and civilian University Research Fellows to study intensively subjects related to national security. The research results, normally published in monographs, issue papers, or books, are made available to cognizant Government officials and selected activities in the private sector. The directorate also administers the National Security Affairs Institute, which offers opportunities for Government officials to meet with distinguished scholars and other knowledgeable citizens to explore national security issues.

National Security Affairs Monograph Series 83-5
National Defense University Press
Washington, DC 20319

END

DATE
FILMED

10-83

DTI